

ỦY BAN NHÂN DÂN TỈNH BÌNH DƯƠNG
TRƯỜNG CAO ĐẲNG NGHỀ VIỆT NAM - SINGAPORE

GIÁO TRÌNH

**Mô đun: CẤU HÌNH VÀ QUẢN TRỊ
THIẾT BỊ MẠNG**

NGHỀ: QUẢN TRỊ MẠNG MÁY TÍNH
TRÌNH ĐỘ TRUNG CẤP NGHỀ

*Ban hành kèm theo Quyết định số: /QĐ-TCĐNVS ngày tháng năm
của Trường Cao đẳng nghề Việt Nam - Singapore*

Bình Dương, năm 2020

LỜI GIỚI THIỆU

Qua thời gian giảng dạy tại trường Cao đẳng nghề Việt Nam-Singapore cùng với các thầy/cô trong khoa Tin học và Đại cương, bản thân tôi thấy cần biên soạn lại giáo trình về mô đun; cấu hình và quản trị thiết bị mạng nhằm đáp ứng với chương trình giảng dạy hệ trung cấp nghề quản trị mạng máy tính. Giáo trình biên soạn lại sẽ phù hợp với chương trình và mô đun: cấu hình và quản trị thiết bị mạng đã được điều chỉnh năm 2019.

Giáo trình, trình bày về lý thuyết và các bước thực hành, thiết lập kết nối bằng HyperTerminal vào router, chuyển đổi giữa các chế độ cấu hình router, thiết lập IP cho các cổng của Router, cấu hình và định tuyến được router, thực hiện được chính sách bảo mật trên Router... Với mong muốn tìm hiểu kỹ về công nghệ thông tin, mạng máy tính để có thể xây dựng, ứng dụng tối đa các tiện ích mà mạng máy tính mang lại sau khi học mô đun cấu hình và quản trị thiết bị mạng. Trong quá trình biên soạn giáo trình này, dù đã cố gắng nhiều nhưng không thể tránh được những thiếu sót. Rất mong được sự góp ý của quý thầy/cô để giáo trình này được hoàn chỉnh hơn.

Giáo trình này được biên soạn lại từ những nguồn tài liệu tham khảo khác nhau cho phù hợp với chương trình và điều kiện giảng dạy tại Trường Cao đẳng nghề Việt Nam- Singapore và chỉ lưu hành nội bộ.

Bình Dương, ngày 08 tháng 04 năm 2020

NGUYỄN ANH TUẤN- Tác giả

MỤC LỤC

MỤC LỤC.....	3
DANH MỤC THUẬT NGỮ VIẾT TẮT.....	9
DANH MỤC HÌNH ẢNH	10
DANH MỤC BẢNG BIỂU	15
CHƯƠNG TRÌNH MÔ ĐUN	17
BÀI 1:WAN VÀ ROUTER	19
1. WAN.	19
1.1 Giới thiệu về WAN.	19
1.2 Giới thiệu về router trong mạng WAN.	20
1.3 Router LAN và WAN.	22
1.4 Vai trò của các router trong WAN.....	23
2. Router.....	25
2.1 Các thành phần bên trong router.....	25
2.2 Đặc điểm vật lý của router.	26
2.3 Các loại kết nối bên ngoài của router	27
2.4 Kết nối vào cổng quản lý trên router.	28
2.5 Thiết lập kết nối vào cổng console	28
3.BÀI TẬP THỰC HÀNH 1.1.....	30
3.1. Mô hình	30
3.2.Yêu cầu:.....	30
3.3.Chuẩn bị:	30
3.4.Các bước thực hành:.....	30
3.5. Những sự cố thường gặp	37
3.6. Báo cáo kết quả thực hành	37
3.7. Đánh giá các bước thực hành	38
4.TÓM TẮT NỘI DUNG	38
5.CÂU HỎI VÀ BÀI TẬP	38
BÀI 2:GIỚI THIỆU VỀ ROUTER.....	40
1. Giới thiệu hệ điều hành IOS.....	40
1.1 Mục đích của phần mềm IOS.....	40
1.2 Giao diện người dùng của router.	40
1.3 Các chế độ cấu hình router.....	41
2. Các đặc điểm và hoạt động của phần mềm IOS	42
2.1 Các đặc điểm của phần mềm IOS	42
2.2 Hoạt động của phần mềm IOS	44
2.3 Khởi động router.....	45
2.4 Đèn LED báo hiệu trên router.....	47
2.5 Khảo sát quá trình khởi động router.	47
2.6 Thiết lập phiên kết nối bằng HyperTerminal.....	49
2.7 Truy cập vào router.....	49
2.8 Phím trợ giúp trong router CLI	50

2.9 Mở rộng thêm về cách viết câu lệnh.....	51
2.10 Gọi lại các lệnh đã sử dụng.....	52
2.11 Xử lý lỗi câu lệnh.....	52
2.12 Lệnh show version	53
3.BÀI TẬP THỰC HÀNH 2.1	54
3.1.Mô hình	54
3.2. Yêu cầu.....	54
3.3.Chuẩn bị	55
3.4.Các bước thực hành:.....	55
3.5.Những sự cố thường gặp	57
3.6.Báo cáo kết quả thực hành	58
3.7.Đánh giá các bước thực hành	58
4.TÓM TẮT NỘI DUNG	59
5.CÂU HỎI VÀ BÀI TẬP	59
BÀI 3:CẤU HÌNH ROUTER	60
1. Cấu hình router.....	60
1.1 Chế độ giao tiếp dòng lệnh CLI.....	60
1.2 Đặt tên cho router.....	61
1.3 Đặt mật mã cho router.....	61
1.4 Kiểm tra bằng các lệnh show	62
1.5 Cấu hình cổng serial.....	63
1.6 Thêm bớt, dịch chuyển và thay đổi tập tin cấu hình.....	64
1.7 Cấu hình cổng Ethernet.....	65
2. Hoàn chỉnh cấu hình router.....	65
2.1 Tầm quan trọng của việc chuẩn hoá tập tin cấu hình	65
2.2 Câu chú thích cho các cổng giao tiếp	66
2.3 Cấu hình câu chú thích cho cổng giao tiếp	66
2.4 Thông điệp đăng nhập.Cấu hình thông điệp đăng nhập (MOTD).....	67
2.5 Phân giải tên máy	68
2.6 Cấu hình bằng host.....	68
2.7 Lập hồ sơ và lưu dự phòng tập tin cấu hình	69
2.8 Cắt, dán và chỉnh sửa tập tin cấu hình	69
3.BÀI TẬP THỰC HÀNH 3.1	70
3.1.Mô hình	70
3.2.Yêu cầu.....	70
3.3.Chuẩn bị:	70
3.4.Các bước thực hành:.....	71
3.5.Những sự cố thường gặp	73
3.6.Báo cáo kết quả thực hành	74
3.7.Đánh giá các bước thực hành	74
4.TÓM TẮT NỘI DUNG	75
5.CÂU HỎI VÀ BÀI TẬP	75
BÀI 4:CẬP NHẬT THÔNG TIN TỪ CÁC THIẾT BỊ KHÁC	76
1. Kết nối và khám phá các thiết bị lân cận.	76
1.1 Giới thiệu về CDP	76

1.2	Thông tin thu nhận được từ CDP	76
1.3	Chạy CDP, kiểm tra và ghi nhận các thông tin CDP	77
1.4	Xây dựng bản đồ mạng	78
1.5	Tắt CDP	78
1.6	Xử lý sự cố của CDP	79
2.	Thu thập thông tin về các thiết bị ở xa	79
2.1	Telnet	79
2.2	Thiết lập và kiểm tra quá trình khởi động router	80
2.3	Ngắt, tạm ngưng phiên Telnet	80
2.4	Mở rộng thêm về hoạt động Telnet	81
2.5	Các lệnh kiểm tra kết nối khác	82
2.6	Xử lý sự cố về địa chỉ IP	83
3.	BÀI TẬP THỰC HÀNH 4.1	83
3.1.	Mô hình	83
3.2.	Yêu cầu	83
3.3.	Chuẩn bị:	84
3.4.	Các bước thực hành:	84
3.5.	Những sự cố thường gặp	85
3.6.	Báo cáo kết quả thực hành	86
3.7.	Đánh giá các bước thực hành	86
4.	TÓM TẮT NỘI DUNG	87
5.	CÂU HỎI VÀ BÀI TẬP	87
BÀI 5:	QUẢN LÝ PHẦN MỀM IOS	88
1.	Khảo sát và kiểm tra hoạt động router	88
1.1	Các giai đoạn khởi động router khi bắt đầu bật điện	88
1.2	Thiết bị Cisco tìm và tải IOS như thế nào	89
1.3	Sử dụng lệnh boot system	89
1.4	Thanh ghi cấu hình	90
1.5	Xử lý sự cố khi khởi động IOS	90
2.	Quản lý tập tin hệ thống	90
2.1	Khái quát về tập tin hệ thống IOS	90
2.2	Quy ước tên IOS	91
2.3	Quản lý tập tin cấu hình bằng TFTP	92
2.4	Quản lý tập tin cấu hình bằng cách cắt-dán	93
2.5	Quản lý Cisco IOS bằng TFTP	95
2.6	Quản lý IOS bằng Xmodem	95
2.7	Biến môi trường	97
2.8	Kiểm tra tập tin hệ thống	99
3.	BÀI TẬP THỰC HÀNH 5.1	99
3.1.	Mô hình	99
3.2.	Yêu cầu:	99
3.3.	Chuẩn bị:	99
3.4.	Các bước thực hành:	99
3.5.	Những sự cố thường gặp	106
3.6.	Báo cáo kết quả thực hành	107

3.7.Đánh giá các bước thực hành	107
4.TÓM TẮT NỘI DUNG	108
5.CÂU HỎI VÀ BÀI TẬP	109
BÀI 6:ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN	110
1. Giới thiệu về định tuyến tĩnh.	110
1.1 Giới thiệu về định tuyến tĩnh	110
1.2 Hoạt động của định tuyến tĩnh.....	110
1.3 Cấu hình đường cố định.....	112
1.4 Cấu hình đường mặc định cho router chuyển gói đi	113
1.5 Kiểm tra cấu hình.....	114
1.6 Xử lý sự cố	115
2. Tổng quát về định tuyến	115
2.1 Giới thiệu về giao thức định tuyến	115
2.2 Autonomous system (AS) (Hệ thống tự quản)	115
2.3 Mục đích của giao thức định tuyến và hệ thống tự quản.....	116
2.4 Phân loại các giao thức định tuyến	116
2.5 Đặc điểm của giao thức định tuyến theo vector khoảng cách	117
2.6 Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết..	117
2.7 Quyết định chọn đường đi	119
2.8 Cấu hình định tuyến	119
2.9 Các giao thức định tuyến	119
2.10 Hệ tự quản, IGP và EGP	121
2.11 Trạng thái đường liên kết.....	121
3.BÀI TẬP THỰC HÀNH 6.1.....	122
3.1.Mô hình	122
3.2.Yêu cầu.....	122
3.3.Chuẩn bị:	123
3.4.Các bước thực hành:.....	123
3.5.Những sự cố thường gặp	124
3.6.Báo cáo kết quả thực hành	124
3.7.Đánh giá các bước thực hành.....	125
4.TÓM TẮT NỘI DUNG	125
5.CÂU HỎI VÀ BÀI TẬP	126
BÀI 7: GIAO THỨC ĐỊNH TUYẾN THEO VECTOR KHOẢNG CÁCH....	127
1. Định tuyến theo vector khoảng cách.....	127
1.1 Cập nhật thông tin định tuyến.....	127
1.2 Định nghĩa giá trị tối đa	127
1.3 Tránh định tuyến lặp vòng bằng split horizon.....	128
1.4 Router poisoning.....	129
1.5 Tránh định tuyến lặp vòng bằng cơ chế cập nhật tức thời.....	130
1.6 Tránh lặp vòng với Thời gian holddown	131
2. RIP.....	131
2.1 Tiến trình của RIP	131
2.2 Cấu hình RIP	132
2.3 Sử dụng lệnh ip classless	134

2.4	Những vấn đề thường gặp khi cấu hình RIP.....	135
2.5	Kiểm tra cấu hình RIP.....	137
2.6	Xử lý sự cố về hoạt động cập nhật của RIP.....	139
2.7	Ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp 140	
2.8	Chia tải với RIP.....	141
2.9	Chia tải cho nhiều đường.....	142
2.10	Tích hợp đường cố định với RIP	143
2.11	Đặc điểm của IGRP	145
2.12	Kiểm tra cấu hình IGPR.....	145
2.13	Xử lý sự cố của IGPR	146
3.	BÀI TẬP THỰC HÀNH 7.1.....	146
3.1.	Mô hình	146
3.2.	Yêu cầu.....	147
3.3.	Chuẩn bị:	147
3.4.	Các bước thực hành:.....	147
3.5.	Những sự cố thường gặp	149
3.6.	Báo cáo kết quả thực hành	149
3.7.	Đánh giá các bước thực hành.....	149
4.	TÓM TẮT NỘI DUNG	150
5.	CÂU HỎI VÀ BÀI TẬP.....	150
BÀI 8:	THÔNG điệp ĐIỀU KHIỂN VÀ BÁO LỖI CỦA TCP/IP	152
1.	Tổng quát về thông điệp báo lỗi của TCP/IP Cách thức.	152
1.1	Giao thức thông điệp điều khiển Internet (IMCP).....	152
1.2	Truyền thông điệp IMCP	152
1.3	Mạng không đến được	153
1.4	Sử dụng lệnh ping để kiểm tra xem địa chỉ đích có đến được hay không	153
1.5	Phát hiện đường dài quá giới hạn	154
1.6	Thông điệp echo.....	155
1.7	Thông điệp “Destination Unreachable”.....	155
1.8	Thông báo các loại lỗi khác	155
2.	Thông điệp điều khiển của TCP/IP.....	156
2.1	Giới thiệu về thông điệp điều khiển.....	156
2.2	Thông điệp ICMP redirect/change request	157
2.3	Đồng bộ đồng hồ và ước tính Thời gian truyền dữ liệu	158
2.4	Thông điệp Information request và reply	159
2.5	Thông điệp để tìm router.....	160
2.6	Thông điệp Router solicitation.....	160
2.7	Thông điệp báo nghẽn và điều khiển luồng dữ liệu.....	161
3.	BÀI TẬP THỰC HÀNH 8.1.....	161
3.1.	Mô hình	161
3.2.	Yêu cầu.....	161
3.3.	Chuẩn bị:	161
3.4.	Các bước thực hành:.....	162

3.5.Những sự cố thường gặp	167
3.6.Báo cáo kết quả thực hành	167
3.7.Đánh giá các bước thực hành	168
4.TÓM TẮT NỘI DUNG	168
5.CÂU HỎI VÀ BÀI TẬP	169
BÀI 9 : CAMERA	170
1.Giới thiệu về camera.....	170
2.Phân loại về camera.....	170
2.1 Phân loại	170
2.2 Công nghệ camera.....	171
3.Bài tập 9.1, thực hành cài đặt, cấu hình camera IP có dây	171
3.1 Sơ đồ hệ thống camera	171
3.2.Yêu cầu.....	172
3.3.Chuẩn bị:	172
3.4.Các bước thực hành.....	173
3.5.Những sự cố thường gặp	176
3.6.Báo cáo kết quả thực hành	177
3.7.Đánh giá các bước thực hành	177
4.Bài tập 9.2, thực hành cài đặt, cấu hình camera IP không dây	177
4.1.Sơ đồ hệ thống camera	177
4.2.Yêu cầu.....	178
4.3.Chuẩn bị:	178
4.4.Các bước thực hành	178
4.4.1.Cài đặt và cấu hình Camera trên điện thoại Smart phone:	178
4.4.2. Cài đặt xem camera Kbvision cho máy tính.	181
4.5.Những sự cố thường gặp.	184
4.6.Báo cáo kết quả thực hành	187
4.7.Đánh giá các bước thực hành	188
5.TÓM TẮT NỘI DUNG	189
6.CÂU HỎI VÀ BÀI TẬP	189
TÀI LIỆU THAM KHẢO	191

DANH MỤC THUẬT NGỮ VIẾT TẮT

ICMP	Viết tắt của Internet Control Message Protocol. Đây là giao thức xử lý các thông báo trạng thái
Telnet	Viết tắt của TErminaL NETwork là một giao thức mạng
DNS	Viết tắt của Domain Name System. Hệ thống tên miền
SMTP	Viết tắt của Simple Message Transfer Protocol. Giao thức SMTP dùng để gửi thư
CGI	Viết tắt của Common Gateway Interface. Giao diện công chung
SYN	Viết tắt của The Synchronous Idle Character. Ký tự đồng bộ hoá.
LAN	Viết tắt của Local Area Network. Một hệ thống các máy tính và thiết bị ngoại vi được liên kết với nhau.
ISP	Viết tắt của Internet Service Provider. Nhà cung cấp dịch vụ Internet.
IPC	Viết tắt của Inter-Process Communication. Được dùng trong việc chia sẻ dữ liệu giữa các ứng dụng và máy tính trên mạng
SSI	viết tắt của Server Side Includes. Các chỉ dẫn được đặt trong các file html.
ppp	Viết tắt của Point-to-Point. Giao thức kết nối Internet tin cậy thông qua Modem
OSI	Viết tắt của Open System Interconnection. Mô hình chuẩn
ATM	Viết tắt của Asynchronous Transfer Mode. Kỹ thuật mạng định hướng
DHCP	Viết tắt của Dynamic Host Configuration Protocol. Giao thức mà máy sử dụng để lấy được tất cả thông tin cấu hình cần thiết, bao gồm cả địa chỉ IP
SMB	Viết tắt của Server Message Block. Protocols phổ biến cho PC

DANH MỤC HÌNH ẢNH

Hình 1. 1: các thiết bị WAN	20
Hình 1. 2: Router Cisco 1841	20
Hình 1. 3: Phân đoạn mạng LAN với router.....	22
Hình 1. 4: Kết nối router bằng các công nghệ WAN.....	22
Hình 1. 5: Vùng WAN.....	23
Hình 1. 6: Các chuẩn WAN ở lớp vật lý.....	24
Hình 1. 7: Các kiểu đóng gói dữ liệu WAN ở lớp liên kết dữ liệu	24
Hình 1. 8: Các cổng giao tiếp	26
Hình 1. 9: Cổng giao tiếp trong main board	26
Hình 1. 10: Cấu trúc bên trong của router 1841	27
Hình 1. 11: Các loại kết nối bên ngoài của router 1841	27
Hình 1. 12: Kết nối modem vào cổng console hay cổng AUX.....	29
Hình 1. 13: Mô hình PC kết nối với router	30
Hình 1. 14: Khởi động phần mềm.....	30
Hình 1. 15: Check chọn I accept the agreement và Next.....	31
Hình 1. 16: Chọn vị trí lưu, nhấn Browse... nếu muốn thay đổi, sau đó.....	31
Hình 1. 17: Chọn Next.....	32
Hình 1. 18: Chọn install.....	32
Hình 1. 19: Chờ quá trình cài đặt diễn ra	33
Hình 1. 20: Chọn finish	33
Hình 1. 21: Chọn Router 1841 và kéo ra giữa giao diện	34
Hình 1. 22: Chọn PC-PT và kéo ra giữa giao diện	34
Hình 1. 23: Chọn Connections và chọn dây Console	35
Hình 1. 24: Chọn đầu RS 232 với PC-PT	35
Hình 1. 25: Với Router ta chọn cổng Console	36
Hình 1. 26: Nhấn vào PC, chọn Desktop sau đó chọn Terminal.....	36
Hình 1. 27: Chỉnh về các thông số sau: 96000 baud, 8 data bits, 1 stop bit, no flow control.....	37
Hình 2. 1: Các chế độ cấu hình Router	41
Hình 2. 2: Lệnh show version.....	44
Hình 2. 3: 3 chế độ hoạt động.....	44
Hình 2. 4: Lệnh show flash	45
Hình 2. 5: Các bước khởi động router	45
Hình 2. 6: Chế độ cài đặt của router.....	47
Hình 2. 7: Báo hiệu đèn LED.....	47
Hình 2. 8: Thông tin hiển thị trong quá trình khởi động router	47
Hình 2. 9: Chế độ cấu hình	48
Hình 2. 10: Hiển thị thông tin phiên bản của bootstrap và IOS	48
Hình 2. 11: Chế độ EXEC đặc quyền.....	50
Hình 2. 12: Danh sách lệnh sử dụng ở chế độ EXEC đặt quyền.....	50
Hình 2. 13: Hiển thị do lệnh show version.....	54

Hình 2. 14: Mô hình PC kết nối Router	54
Hình 2. 15: Chọn CLI sẽ thấy thông tin quá trình khởi động router	55
Hình 2. 16: Chế độ cấu hình router	55
Hình 2. 17: cấu hình cho Router	56
Hình 2. 18: Gõ lệnh clock set + thời gian ngày tháng năm.....	56
Hình 2. 19: Gõ lệnh Router>show version từ giao diện CLI	57
Hình 2. 20: Gõ lệnh Router>show flash từ giao diện CLI	57
Hình 3. 1: Giao diện dòng lệnh.....	60
Hình 3. 2: Lệnh đặt passrord	62
Hình 3. 3: Lệnh show running- config	65
Hình 3. 4: Lệnh shutdown	65
Hình 3. 5: Câu chú thích cho các cổng giao tiếp.....	66
Hình 3. 6: Thông điệp đăng nhập	67
Hình 3. 7: Cấu hình đăng nhập.....	68
Hình 3. 8: Mô hình PC kết nối Router	70
Hình 3. 9: Giao diện khi nhấn vào Router A	71
Hình 3. 10: Giao diện khi nhấn vào Router A	71
Hình 3. 11: Đặt mật mã cho Router A	72
Hình 3. 12: Cấu hình cổng Serial	72
Hình 3. 13: Cấu hình câu chú thích cho cổng Serial.....	73
Hình 3. 14: Sao chép tập tin trên Router A.....	73
Hình 4. 1: Lệnh no cdp enable	78
Hình 4. 2: Telnet hoạt động ở lớp ứng dụng	79
Hình 4. 3: Telnet ở 2 vùng.....	80
Hình 4. 4: Trình tự Telnet	81
Hình 4. 5: Tổ hợp phím Ctrl- Shift-6, x	82
Hình 4. 6: :Lệnh kiểm tra kết nối	82
Hình 4. 7: Mô hình PC kết nối Router	83
Hình 4. 8: Giao diện khi nhấn vào Router A	84
Hình 4. 9: Lệnh CDP run	84
Hình 4. 10: Lệnh no CDP run.....	85
Hình 4. 11: Hiển thị thông tin địa chỉ ip trên Router	85
Hình 4. 12: Hiển thị các mạng kết nối trực tiếp vào Router	85
Hình 5. 1: tập tin hệ thống	91
Hình 5. 2: Quá trình chép tập tin bằng kết nối HyperTerminal	94
Hình 5. 3: Quá trình chép tập tin cấu hình vào router bằng kết nối HyperTerminal	95
Hình 5. 4: Lệnh copy tftp flash	95
Hình 5. 5: Lệnh confreg	96
Hình 5. 6: Lệnh Xmodem.....	97
Hình 5. 7: Cửa sổ Send File	98

Hình 5. 8: Mô hình Router kết nối Server	99
Hình 5. 9: Khởi động phần mềm Cisco Packet Tracer	100
Hình 5. 10: Chọn thiết bị Router và Server	100
Hình 5. 11: Chọn cổng FastEthernet0/0	100
Hình 5. 12: Chọn cổng FastEthernet0	100
Hình 5. 13: Chuyển sang chế độ đặt quyền	101
Hình 5. 14: Cấu hình địa chỉ IP và Subnet Mask cho Router.....	101
Hình 5. 15: Chọn IP Configuration	102
Hình 5. 16: Nhập địa chỉ IP, Subnet và Default Gateway cho Server.....	102
Hình 5. 17: Chọn Command Prompt	103
Hình 5. 18: Ping Server qua Router.....	103
Hình 5. 19: Ping Router qua Server.....	104
Hình 5. 20: : Lưu file cấu hình từ DRAM vào NVRAM	104
Hình 5. 21: Bật dịch vụ TFTP trên máy chủ TFTP Server	104
Hình 5. 22: Copy IOS image mới vào bộ nhớ Flash của Router	105
Hình 5. 23: Đặt biến khởi động cho Router và ghi cấu hình.....	105
Hình 5. 24: : Kiểm tra bằng lệnh show running-config.....	105
Hình 5. 25: Tải lại Router	106
Hình 5. 26: Kiểm tra lại system image file name IOS mới	106
Hình 6. 1: Lệnh iproute.....	111
Hình 6. 2: Cấu hình đường đi cố định	111
Hình 6. 3: Câu lệnh chỉ cho router biết địa chỉ IP của router kế tiếp	111
Hình 6. 4: Cấu hình đường đi cố định	113
Hình 6. 5: Một AS là bao gồm các router hoạt động dưới cùng một cơ chế quản trị	116
Hình 6. 6: Router A nhận được thông tin về các mạng khác từ router B.....	117
Hình 6. 7: : router chọn đường cho gói dữ liệu	119
Hình 6. 8: hệ tự quản IRP và EGP.....	121
Hình 6. 9: Mô hình PC kết nối Router	122
Hình 6. 10: Nhấn vào giao diện Router CNTT	123
Hình 6. 11: Sử dụng lệnh ip route để cấu hình đường cố định.....	124
Hình 6. 12: Cấu hình RIP	124
Hình 7. 1: bảng định tuyến.....	127
Hình 7. 2: Thông số định tuyến	128
Hình 7. 3: Cơ chế split-horizon.....	129
Hình 7. 4: Thông tin route poisonin	130
Hình 7. 5: Cơ chế cập nhật tức thời.....	131
Hình 7. 6: Cấu hình RIP.....	133
Hình 7. 7: khi không có lệnh ip classless.....	134
Hình 7. 8: khi có lệnh ip classless	135
Hình 7. 9: Thời gian cập nhật router	136
Hình 7. 10: Lệnh show ip protocols	138

Hình 7. 11: Lệnh show ip router	138
Hình 7. 12: lệnh debug ip rip	139
Hình 7. 13: Subnet không liên tục	139
Hình 7. 14: Trùng Subnet.....	140
Hình 7. 15: Lệnh passive interface	141
Hình 7. 16: RIP chia tải ra 4 đường có chi phí bằng nhau	141
Hình 7. 17: Lệnh show ip route.....	142
Hình 7. 18: router có thể chia tải là từ 1 đến 6 đường	142
Hình 7. 19: router sẽ sử dụng đường mặc định.....	143
Hình 7. 20: Cấu hình chỉ số AD.....	144
Hình 7. 21: Cấu hình chỉ số AD khi bị sự cố	144
Hình 7. 22: Lệnh Debug ip igrp events	146
Hình 7. 23: Mô hình PC kết nối Router	146
Hình 7. 24: Chuyển sang tab CLI	147
Hình 7. 25: Chuyển sang chế độ toàn cục	147
Hình 7. 26: Cấu hình RIP cổng FastEthernet 0/0.....	148
Hình 7. 27: Cấu hình RIP cổng Serial 2/0.....	148
Hình 7. 28: Cấu hình RIP cho RouterCoKhi	148
Hình 7. 29: Cấu hình RIP cho RouterDienTu.....	149
Hình 8. 1: Thông điệp ICMP.....	153
Hình 8. 2: router gửi thông điệp ICMP	153
Hình 8. 3: : Lệnh ping gửi đi 4 gói echo request	154
Hình 8. 4: Lệnh ping địa chỉ IP.....	154
Hình 8. 5: Thông điệp “Destination Unreachable”.....	155
Hình 8. 6: Thông điệp “Parameter Problem”	156
Hình 8. 7: : Một số thông điệp ICMP	156
Hình 8. 8: Thông điệp ICMP redirect/change request	157
Hình 8. 9: Host H nên sử dụng Router R2 làm gateway.....	158
Hình 8. 10: Thông điệp hỏi giờ.....	159
Hình 8. 11: Cấu trúc của thông điệp Address Mask Request và reply.....	160
Hình 8. 12: Cấu trúc của thông tin điệp Router advertisement	160
Hình 8. 13: Cấu trúc của thông điệp Router solicitation	160
Hình 8. 14: Mô hình PC kết nối Router	161
Hình 8. 15: Chuyển sang tab Desktop	162
Hình 8. 16: Chọn IP Configuration	162
Hình 8. 17: Nhập các địa chỉ IP, Subnet Mask và Default GateWay cho PC1 .	163
Hình 8. 18: Nhập các địa chỉ IP, Subnet Mask và Default GateWay cho PC2 .	163
Hình 8. 19: Chuyển sang tab CLI	164
Hình 8. 20: Chuyển sang chế độ toàn cục	164
Hình 8. 21: Cấu hình RIP cổng FastEthernet 0/0.....	164
Hình 8. 22: Cấu hình RIP cổng Serial 2/0.....	165
Hình 8. 23: Cấu hình RIP cho RouterCoKhi	165
Hình 8. 24: Cấu hình RIP cho RouterDienTu.....	165

Hình 8. 25: Chuyển sang tab Desktop	166
Hình 8. 26: Chọn Cammand Prompt	166
Hình 8. 27: Ta gõ lệnh ping +địa chỉ ip của pc3.....	166
Hình 8. 28: Ta gõ lệnh ping +địa chỉ ip của pc6.....	167
Hình 9. 1: các loại camera.....	170
Hình 9. 2: hệ thống camera IP sử dụng dây cáp mạng	172
Hình 9. 3: màn hình chính của main menu	174
Hình 9. 4: giao diện nhập thông tin	175
Hình 9. 5: giao diện màn hình nền.....	175
Hình 9. 6: : Cách set up đầu ghi xem camera từ xa	175
Hình 9. 7: : bật chế độ DHCP.....	176
Hình 9. 8: chế độ xem camera	176
Hình 9. 9: hệ thống camera sử dụng wifi.....	178
Hình 9. 10: giao diện giám sát camera.....	178
Hình 9. 11: màn hình camera xem trực tiếp	179
Hình 9. 12: : màn hình quản lý thiết bị	179
Hình 9. 13: màn hình cài đặt quản lý thiết bị	179
Hình 9. 14: menu thêm thiết bị.....	180
Hình 9. 15: các chế độ xem hình ảnh.....	180
Hình 9. 16: : cài đặt chế độ xem hình ảnh có DNS	181
Hình 9. 17: màn hình đăng nhập	182
Hình 9. 18: giao diện vào màn hình chính.....	182
Hình 9. 19: giao diện cài đặt màn hình xem camera	182
Hình 9. 20: xem camera bằng mã Cloud	183
Hình 9. 21: Save and Continue	184

DANH MỤC BẢNG BIỂU

<i>Bảng 1. 1: Chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 1.1</i>	30
<i>Bảng 1. 2: những sự cố thường gặp của bài tập 1.1.....</i>	37
<i>Bảng 1. 3: đánh giá các bước thực hành bài tập 1.1.....</i>	38
<i>Bảng 2. 1: Các đặt điểm của phần mềm IOS.....</i>	42
<i>Bảng 2. 2: tổ hợp phím.....</i>	51
<i>Bảng 2. 3: Giải thích lệnh.....</i>	52
<i>Bảng 2. 4: Chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 2.1</i>	55
<i>Bảng 2. 5: những sự cố thường gặp của bài tập 2.1.....</i>	57
<i>Bảng 2. 6: đánh giá các bước thực hành bài tập 2.1.....</i>	58
<i>Bảng 3. 1: chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 3.1</i>	70
<i>Bảng 3. 2: những sự cố thường gặp của bài tập 3.1.....</i>	73
<i>Bảng 3. 3: đánh giá các bước thực hành bài tập 3.1.....</i>	74
<i>Bảng 4. 1: thông tin CDP.....</i>	77
<i>Bảng 4. 2: mô tả lệnh CDP.....</i>	79
<i>Bảng 4. 3: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 4.1.....</i>	84
<i>Bảng 4. 4: những sự cố thường gặp của bài tập 4.1.....</i>	86
<i>Bảng 4. 5: đánh giá các bước thực hành bài tập 4.1.....</i>	86
<i>Bảng 5. 1: chuẩn bị phần cài đặt, máy tính, router thực hành bài tập 5.1.....</i>	99
<i>Bảng 5. 2: những sự cố thường gặp của bài tập 5.1.....</i>	106
<i>Bảng 5. 3: đánh giá các bước thực hành bài tập 5.1.....</i>	107
<i>Bảng 6. 1: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 6.1.....</i>	123
<i>Bảng 6. 2: những sự cố thường gặp của bài tập 6.1.....</i>	124
<i>Bảng 6. 3: đánh giá các bước thực hành bài tập 6.1.....</i>	125
<i>Bảng 7. 1: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 7.1.....</i>	147
<i>Bảng 7. 2: những sự cố thường gặp của bài tập 7.1.....</i>	149
<i>Bảng 7. 3: đánh giá các bước thực hành bài tập 7.1.....</i>	149
<i>Bảng 8. 1: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 8.1.....</i>	161
<i>Bảng 8. 2: những sự cố thường gặp của bài tập 8.1.....</i>	167
<i>Bảng 8. 3: đánh giá các bước thực hành bài tập 8.1.....</i>	168
<i>Bảng 9. 1: chuẩn bị thiết bị, vật tư thực hành bài tập 9.1.....</i>	172
<i>Bảng 9. 2: những sự cố thường gặp của bài tập 9.1.....</i>	176
<i>Bảng 9. 3: đánh giá các bước thực hành bài tập 9.1.....</i>	177

<i>Bảng 9. 4: chuẩn bị thiết bị thực hành bài tập 9.2</i>	<i>178</i>
<i>Bảng 9. 5:những sự cố thường gặp của bài tập 9.2.....</i>	<i>184</i>
<i>Bảng 9. 6: đánh giá các bước thực hành bài tập 9.2.....</i>	<i>188</i>

CHƯƠNG TRÌNH MÔ ĐUN

CẤU HÌNH VÀ QUẢN TRỊ THIẾT BỊ MẠNG

Mã mô đun: MD28

Thời gian mô đun: 75 giờ; (Lý thuyết: 30 giờ; Thực hành: 45 giờ)

I. VỊ TRÍ, TÍNH CHẤT CỦA MÔ ĐUN:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong môn, mô đun: Mạng máy tính và quản trị mạng 1, quản trị mạng 2, an toàn mạng
- Tính chất: Là mô đun chuyên ngành bắt buộc.

II. MỤC TIÊU MÔ ĐUN:

- Về kiến thức:
 - + Giải thích sự khác nhau giữa LAN và WAN;
 - + Xác định được các thành phần bên trong Router;
 - + Chuyển đổi giữa các chế độ cấu hình router;
 - + Thiết lập kết nối bằng HyperTerminal vào router;
 - + Sử dụng tính năng trợ giúp trong giao tiếp bằng dòng lệnh;
- Về kỹ năng:
 - + Thiết lập định tuyến cho router.
 - + Cấu hình, quản trị được router, camera
- Về năng lực tự chủ và trách nhiệm: Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập

III. NỘI DUNG MÔ ĐUN

Nội dung tổng quát và phân bổ thời gian

SỐ TT	Tên các bài trong mô đun	Thời gian (giờ)			
		Tổng số	Lý thuyết	Thực hành, thảo luận, bài tập	Kiểm tra
1	Bài 1: WAN và Router	7	3	4	
2	Bài 2: Giới thiệu về Router	7	3	4	
3	Bài 3: Cấu hình Router	10	3	6	1
4	Bài 4: Cập nhật thông tin từ các thiết bị khác	5	2	2	1

5	Bài 5: Quản lý phần mềm IOS	8	3	4	1
6	Bài 6: Định tuyến và các giao thức định tuyến	10	4	6	
7	Bài 7: Giao thức định tuyến theo Vector khoảng cách	8	5	3	
8	Bài 8: Thông điệp điều khiển và báo lỗi của TCP/IP	5	2	2	1
9	Bài 9 : Camera	15	5	10	
	Cộng	75	30	41	4

BÀI 1: WAN VÀ ROUTER

Mã bài MD 28-01

Thời gian: 7 giờ

I. MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Xác định được tổ chức quốc tế chịu trách nhiệm về các chuẩn của WAN;
- Giải thích sự khác nhau giữa LAN và WAN;
- Trình bày vai trò của Router trong WAN;
- Xác định được các thành phần bên trong router;
- Trình bày các đặc điểm vật lý của router;
- Xác định các loại cổng trên router;
- Thực hiện các thao tác an toàn với máy tính;

II. NỘI DUNG CHÍNH

1. WAN.

1.1 Giới thiệu về WAN.

- WAN (Wide Area Network) là mạng truyền dữ liệu qua những vùng địa lý rất rộng lớn như các bang, tỉnh, quốc gia... Các phương tiện truyền dữ liệu trên WAN được cung cấp bởi các nhà cung cấp dịch vụ, ví dụ như các công ty điện thoại.
- Mạng WAN có một số đặc điểm sau:
 - + WAN dùng để kết nối các thiết bị ở cách xa nhau bởi những địa lý lớn.
 - + WAN sử dụng dịch vụ của các công ty cung cấp dịch vụ, ví dụ như: Regional Bell Operating Companies (RBOCs), Sprint, MCI, VPM internet services, Inc., Altantes.net...
 - + WAN sử dụng nhiều loại liên kết nối tiếp khác nhau.
- WAN có một số điểm khác với LAN. Ví dụ như: LAN được sử dụng để kết nối các máy tính đơn lẻ, các thiết bị ngoại vi, các thiết bị đầu cuối và nhiều loại thiết bị khác trong cùng một tòa nhà hay một phạm vi địa lý nhỏ. Trong khi đó WAN được sử dụng để kết nối các chi nhánh của mình, nhờ đó mà thông tin được trao đổi dễ dàng giữa các trung tâm.
- Mạng WAN hoạt động chủ yếu ở lớp Vật lý và lớp Liên kết dữ liệu mô hình OSI. WAN kết nối các mạng LAN lại với nhau. Do đó, WAN thực hiện chuyển đổi các gói dữ liệu giữa các router, switch và các mạng LAN mà nó kết nối.
- Sau đây là các thiết bị được sử dụng trong WAN:
 - Router: cung cấp nhiều dịch vụ khác nhau, bao gồm Internet và các giao tiếp WAN.

- Loại switch được sử dụng trong WAN cung cấp kết nối cho hoạt động thông tin liên lạc bằng thoại video và dữ liệu.
- Modem: bao gồm: giao tiếp với dịch vụ truyền thoại; CSU/DSU (Chanel service units/ Digital service units) để giao tiếp với dịch vụ T1/E1; TA/NT1 (Terminal Adapters /Network Terminal 1) để giao tiếp với dịch vụ ISDN (Integrate Services Digital Network).
- Server thông tin liên lạc: tập trung xử lý cuộc gọi của người dùng.



Hình 1. 1: các thiết bị WAN

- Các giao thức ở lớp Liên kết dữ liệu của mạng WAN mô tả về cách thức mà gói dữ liệu được vận chuyển giữa các hệ thống trên một đường truyền dữ liệu. Các giao thức này được thiết kế cho các dịch vụ chuyển mạch điểm-đến-điểm, đa điểm, đa truy nhập. Ví dụ như: FrameRelay.

- Các tiêu chuẩn của mạng WAN được định nghĩa và quản lý bởi các tổ chức quốc tế sau:

- + Liên hiệp viễn thông quốc tế - lĩnh vực tiêu chuẩn viễn thông – ITUT (International Telecommunication Union-Telecommunication Standardization Sector), trước đây là Ủy ban cố vấn điện thoại và điện tín quốc tế - CCITT (Consultative Committee for International Telegraph and Telephone).
- + Tổ chức quốc tế về tiêu chuẩn – ISO (International Organization for Standardization).
- + Tổ chức đặc trách về kỹ thuật Internet – IETF (Internet Engineering Task Force).
- + Liên hiệp công nghiệp điện tử - EIA (Electronic Industries Association).

1.2 Giới thiệu về router trong mạng WAN.



Hình 1. 2: Router Cisco 1841

- Router là một loại máy tính đặc biệt. Nó cũng có các thành phần cơ bản giống như máy tính: CPU, bộ nhớ, system bus và các cổng giao tiếp. Router kết nối hai hệ thống mạng với nhau và cho phép hai hệ thống này có thể liên lạc với nhau, ngoài ra router còn thực hiện việc chọn lựa đường đi tốt nhất cho dữ liệu.

- Cũng giống như máy tính cần phải có hệ điều hành để chạy các trình ứng dụng thì router cũng cần phải có hệ điều hành để chạy các tập tin cấu hình. Tập tin cấu hình chứa các câu lệnh và các thông số để điều khiển luồng dữ liệu ra vào trên router.

- Các thành phần chính bên trong router bao gồm: bộ nhớ RAM, NVRAM, bộ nhớ flash, ROM và các cổng giao tiếp.

- RAM động (DRAM- Dynamic RAM) có các đặc điểm và chức năng như sau:

- + Lưu bảng định tuyến.
- + Lưu bảng ARP.
- + Có vùng bộ nhớ chuyển mạch nhanh.
- + Cung cấp vùng nhớ đệm cho các gói dữ liệu
- + Duy trì hàng đợi cho các gói dữ liệu.
- + Cung cấp bộ nhớ tạm thời cho tập tin cấu hình của router khi router đang hoạt động.
- + Thông tin trên RAM sẽ bị xóa mất khi router khởi động lại hoặc bị tắt điện.

- Đặc điểm và chức năng của NVRAM:

- + Lưu giữ tập tin cấu hình khởi động của router.
- + Nội dung của NVRAM vẫn được lưu giữ khi router khởi động lại hoặc bị tắt điện

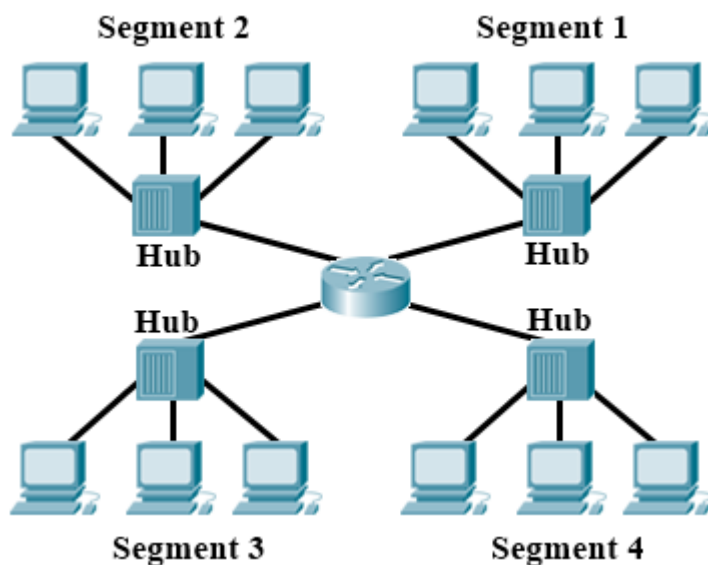
- Đặc điểm và chức năng của bộ nhớ flash:

- + Lưu hệ điều hành IOS.
- + Có thể cập nhật phần mềm lưu trong Flash mà không cần thay đổi chip trên bộ xử lý.
- + Nội dung của Flash vẫn được lưu giữ khi router khởi động lại hoặc bị tắt điện.
- + Ta có thể lưu nhiều phiên bản khác nhau của phần mềm IOS trong Flash.

- Đặc điểm và chức năng của các cổng giao tiếp:

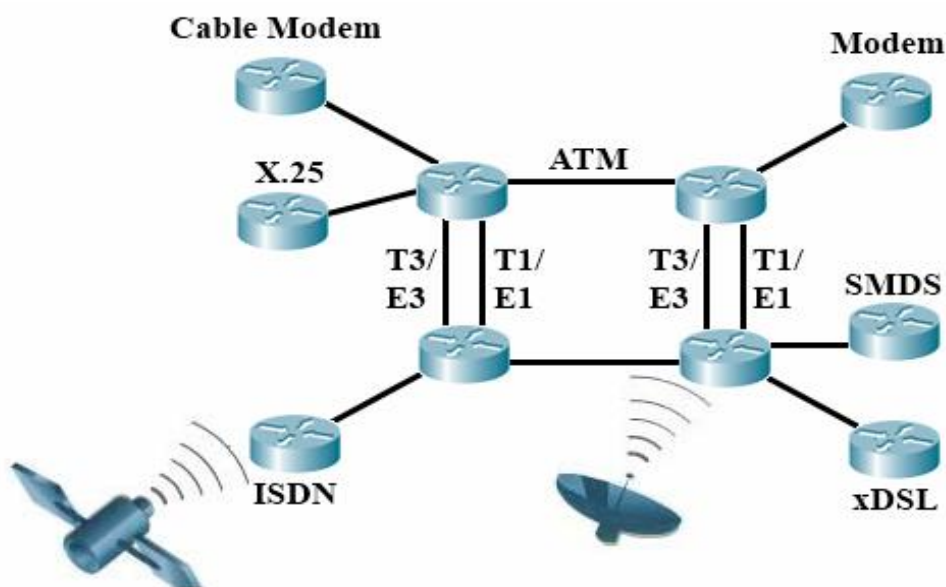
- + Kết nối router vào hệ thống mạng để nhận và chuyển gói dữ liệu.
- + Các cổng có thể gắn trực tiếp trên mainboard hoặc là dưới dạng card rời.

1.3 Router LAN và WAN.



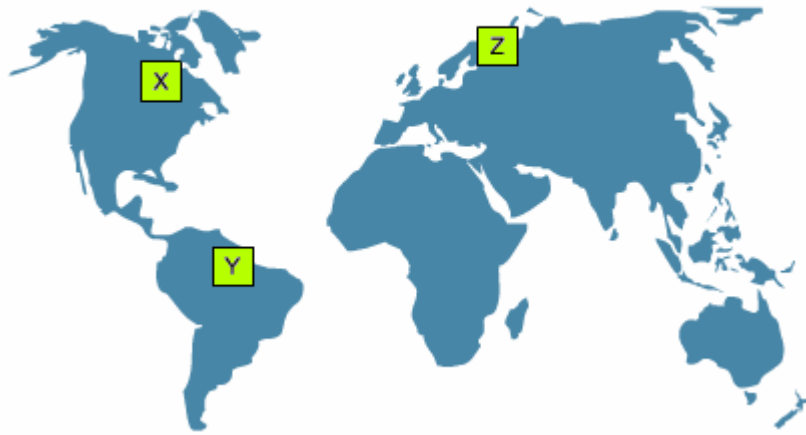
Hình 1. 3: Phân đoạn mạng LAN với router

- Router vừa được sử dụng để phân đoạn mạng LAN vừa là thiết bị chính trong mạng WAN. Do đó, trên router có cả cổng giao tiếp LAN và WAN. Thực chất là các kỹ thuật WAN được sử dụng để kết nối các router, router này giao tiếp với router khác qua đường liên kết WAN. Router là thiết bị xương sống của mạng Intranet lớn và mạng Internet. Router hoạt động ở lớp 3 và thực hiện chuyển gói dữ liệu dựa trên địa chỉ mạng. Router có hai chức năng chính là: chọn đường đi tốt nhất và chuyển mạch gói dữ liệu. Để thực hiện chức năng này, mỗi router phải xây dựng một bảng định tuyến và thực hiện trao đổi thông tin định tuyến với nhau.



Hình 1. 4: Kết nối router bằng các công nghệ WAN

- Người quản trị mạng có thể duy trì bảng định tuyến bằng cách cấu hình định tuyến tĩnh, nhưng thông thường thì bảng định tuyến được lưu giữ động nhờ các giao thức định tuyến thực hiện trao đổi thông tin mạng giữa các router.



Hình 1. 5: Vùng WAN

- Ví dụ: Nếu máy tính X muốn thông tin liên lạc với máy tính Y ở một châu lục khác và với máy tính Z ở một vị trí khác nữa trên thế giới, khi đó cần phải có định tuyến để có thể truyền dữ liệu và đồng thời cũng cần phải có các đường dự phòng, thay thế để đảm bảo độ tin cậy. Rất nhiều thiết kế mạng và công nghệ được đưa ra để cho các máy tính như X, Y, Z có thể liên lạc với nhau.

- Một hệ thống mạng được cấu hình đúng phải có đầy đủ các đặc điểm sau:
 - + Có hệ thống địa chỉ nhất quán từ đầu cuối đến đầu cuối
 - + Cấu trúc địa chỉ phải thể hiện được cấu trúc mạng.
 - + Chọn được đường đi tốt nhất.
 - + Định tuyến động và tĩnh.
 - + Thực hiện chuyển mạch.

1.4 Vai trò của các router trong WAN

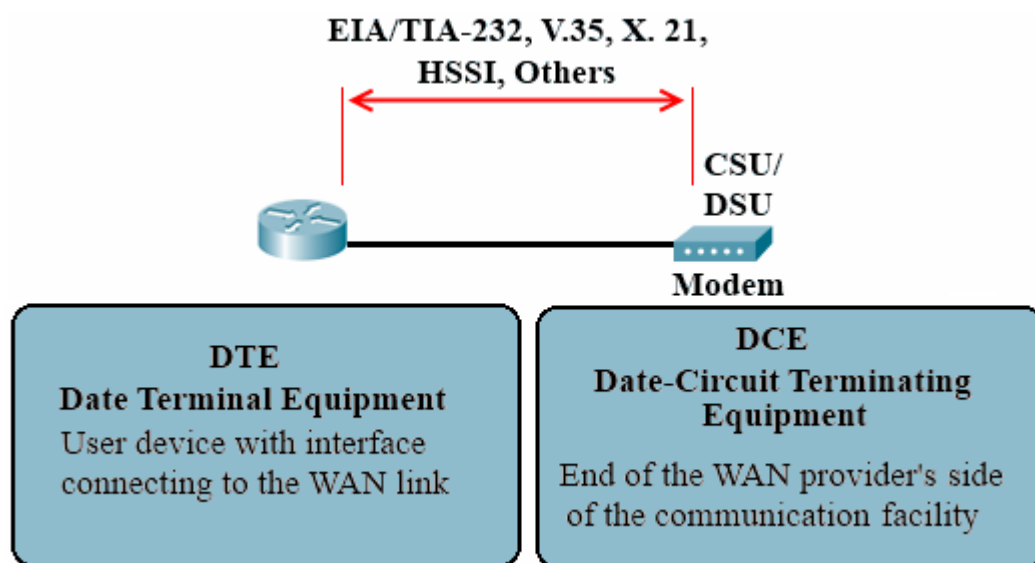
- Mạng WAN hoạt động chủ yếu ở lớp vật lý và lớp liên kết dữ liệu. Điều này không có nghĩa là năm lớp còn lại của mô hình OSI không có trong mạng WAN. Điều này đơn giản có nghĩa là mạng WAN chỉ khác với mạng LAN ở lớp Vật lý và lớp Liên kết dữ liệu. Hay nói cách khác là các tiêu chuẩn và giao thức sử dụng trong mạng WAN ở lớp 1 và lớp 2 là khác với mạng LAN.

- Lớp Vật lý trong mạng WAN mô tả các giao tiếp thiết bị dữ liệu đầu cuối DTE (Data Terminal Equipment) và thiết bị đầu cuối mạch dữ liệu DCE (Data Circuit- terminal Equipment). Thông thường, DCE là thiết bị ở phía nhà cung cấp dịch vụ và DTE là thiết bị kết nối vào DCE. Theo mô hình này thì DCE có thể là modem hoặc CSU/DSU.

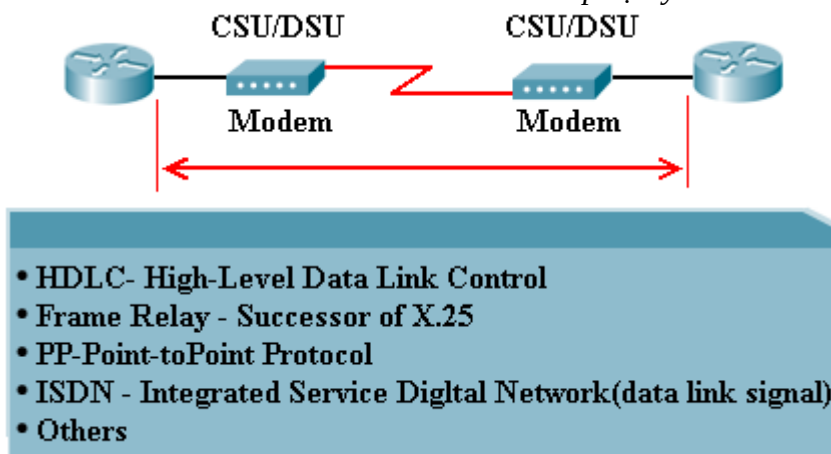
- Chức năng chủ yếu của router là định tuyến. Hoạt động định tuyến diễn ra ở lớp 3 - lớp Mạng trong khi WAN hoạt động ở lớp 1 và 2. Vậy router là thiết bị LAN hay WAN? Câu trả lời là cả hai. Router có thể là thiết bị LAN, hoặc WAN, hoặc thiết bị trung gian giữa LAN và WAN hoặc có thể là LAN và

WAN cùng một lúc.

- Một trong những nhiệm vụ của router trong mạng WAN là định tuyến gói dữ liệu ở lớp 3, đây cũng là nhiệm vụ của router trong mạng LAN. Tuy nhiên, định tuyến không phải là nhiệm vụ chính yếu của router trong mạng WAN. Khi router sử dụng các chuẩn và giao thức của lớp Vật lý và lớp Liên kết dữ liệu để kết nối các mạng WAN thì lúc này nhiệm vụ chính yếu của router trong mạng WAN không phải là định tuyến nữa mà là cung cấp kết nối giữa các mạng WAN với các chuẩn vật lý và liên kết dữ liệu khác nhau. Ví dụ: một router có thể có một giao tiếp ISDN sử dụng kiểu đóng gói PPP và một giao tiếp nối tiếp T1 sử dụng kiểu đóng gói FrameRelay. Router phải có khả năng chuyển đổi luồng bit từ loại dịch vụ này sang dịch vụ khác. Ví dụ: chuyển đổi từ dịch vụ ISDN sang T1, đồng thời chuyển kiểu đóng gói lớp Liên kết dữ liệu từ PPP sang FrameRelay.



Hình 1. 6: Các chuẩn WAN ở lớp vật lý



Hình 1. 7: Các kiểu đóng gói dữ liệu WAN ở lớp liên kết dữ liệu

- Các chuẩn và giao thức WAN lớp vật lý: EIA/TIA-232,449, V24, V35, X21, EIA- 530, ISDN, T1, T3, E1, E3, Xdsl, sonet (oc-3, oc-12, oc-48, oc-192).
- Các chuẩn và giao thức WAN lớp liên kết dữ liệu: HDLC, FrameRelay, PPP, SDLC, SLIP, X25, ATM, LAMB, LAPD, LAPF.

2. Router

2.1 Các thành phần bên trong router

- Cấu trúc chính xác của router rất khác nhau tùy theo từng phiên bản router. Trong phần này chỉ giới thiệu về các thành phần cơ bản của router.

- **CPU:** Đơn vị xử lý trung tâm: thực thi các câu lệnh của hệ điều hành để thực hiện các nhiệm vụ sau: khởi động hệ thống, định tuyến, điều khiển các cổng giao tiếp mạng. CPU là một bộ giao tiếp mạng. CPU là một bộ vi xử lý. Trong các router lớn có thể có nhiều CPU.

- **RAM:** Được sử dụng để lưu bảng định tuyến, cung cấp bộ nhớ cho chuyển mạch nhanh, chạy tập tin cấu hình và cung cấp hàng đợi cho các gói dữ liệu. Trong đa số router, hệ điều hành Cisco IOS chạy trên RAM. RAM thường được chia thành hai phần: phần bộ nhớ xử lý chính và phần bộ nhớ chia sẻ xuất/nhập. Phần bộ nhớ chia sẻ xuất/nhập được chia cho các cổng giao tiếp làm nơi lưu trữ tạm các gói dữ liệu. Toàn bộ nội dung trên RAM sẽ bị xóa khi tắt điện. Thông thường, RAM trên router là loại RAM động (DRAM – Dynamic RAM) và có thể nâng thêm RAM bằng cách gắn thêm DIMM (Dual In-Line Memory Module).

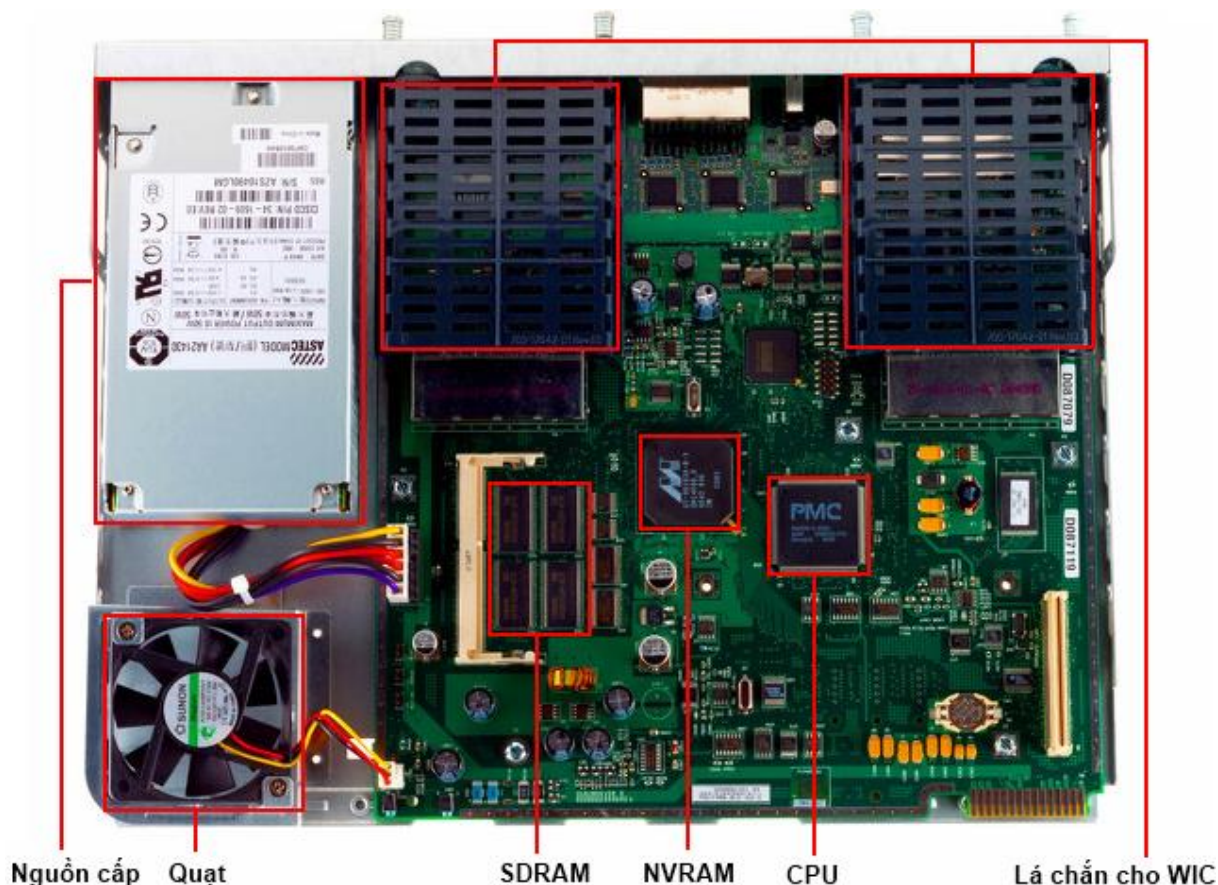
- **Flash:** Bộ nhớ Flash được sử dụng để lưu toàn bộ phần mềm hệ điều hành Cisco IOS. Mặc định là router tìm IOS của nó trong flash. có thể nâng cấp hệ điều hành bằng cách chép phiên bản mới hơn vào flash. Phần mềm IOS có thể ở dưới dạng nén hoặc không nén. Đối với hầu hết các router, IOS được chép lên RAM trong quá trình khởi động router. Còn có một số router thì IOS có thể chạy trực tiếp trên flash mà không cần chép lên RAM có thể gắn thêm hoặc thay thế các thanh SIMM hay card PCMCIA để nâng dung lượng flash.

- **NVRAM** (Non-volatile Random-access Memory): Là bộ nhớ RAM không bị mất thông tin, được sử dụng để lưu tập tin cấu hình.

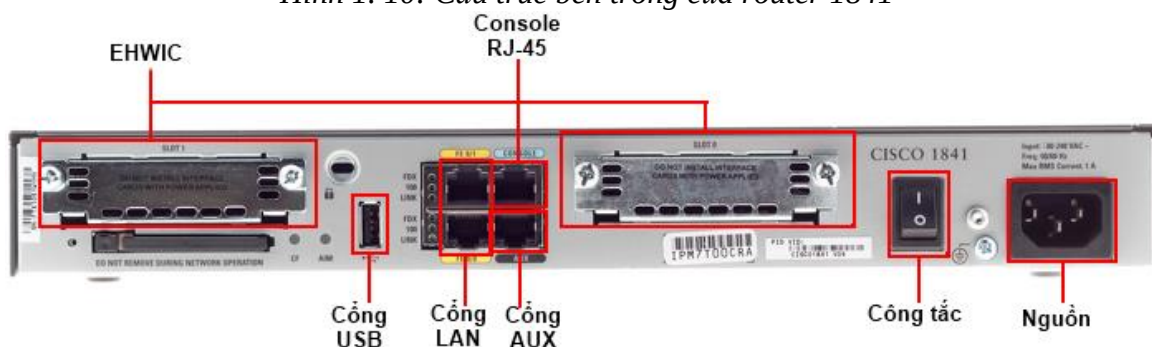
- **Bus:** Phần lớn các router đều có bus hệ thống và CPU bus. Bus hệ thống được sử dụng để thông tin liên lạc giữa CPU với các cổng giao tiếp và các khe mở rộng. Loại bus này vận chuyển dữ liệu và các câu lệnh đi và đến các địa chỉ của ô nhớ tương ứng.

- **ROM** (Read Only Memory): Là nơi lưu đoạn mã của chương trình kiểm tra khi khởi động. Nhiệm vụ chính của ROM là kiểm tra phần cứng của router khi khởi động, sau đó chép phần mềm Cisco IOS từ flash vào RAM. Một số router có thể có phiên bản IOS cũ dùng làm nguồn khởi động dự phòng. Nội dung trong ROM không thể xóa được. Ta chỉ có thể nâng cấp ROM bằng cách thay chip ROM mới.

- **Các cổng giao tiếp:** Là nơi router kết nối với bên ngoài. Router có 3 loại cổng: LAN, WAN và console/AUX. Cổng giao tiếp LAN có thể gắn cố định trên router hoặc dưới dạng card rời.



Hình 1. 10: Cấu trúc bên trong của router 1841



Hình 1. 11: Các loại kết nối bên ngoài của router 1841

2.3 Các loại kết nối bên ngoài của router

- Router có ba loại kết nối cơ bản là: cổng LAN, WAN và cổng quản lý router. Cổng giao tiếp LAN cho phép router kết nối vào môi trường mạng cục bộ LAN. Thông thường, cổng giao tiếp LAN là cổng Ethernet. Ngoài ra cũng có cổng Token Ring và ATM (Asynchronous Transfer Mode).

- Kết nối mạng WAN cung cấp kết nối thông qua các nhà cung cấp dịch vụ đến các chi nhánh ở xa hoặc kết nối vào Internet. Loại kết nối này có thể là nối tiếp hay bất kỳ loại giao tiếp WAN, cần phải có thêm một thiết bị ngoại vi như CSU chẳng hạn để nối router đến nhà cung cấp dịch vụ. Đối với một số loại giao tiếp WAN khác thì có thể kết nối trực tiếp router của mình đến nhà cung cấp dịch vụ.

- Chức năng của port quản lý hoàn toàn khác với ai loại trên. Kết nối LAN, WAN để kết nối router và mạng để router nhận và phát các gói dữ liệu.

Trong khi đó, port quản lý cung cấp cho một kết nối dạng văn bản để có thể cấu hình hoặc xử lý trên router. Cổng quản lý thường là cổng console hoặc cổng AUX (Auxilliary). Đây là loại cổng nối tiếp bất đồng bộ EIA-232. Các cổng này kết nối vào cổng COM trên máy tính. Trên máy tính, chúng ta sử dụng chương trình mô phỏng thiết bị đầu cuối để thiết lập phiên kết nối dạng văn bản vào router. Thông qua kiểu kết nối này, người quản trị mạng có thể quản lý thiết bị của mình.

2.4 Kết nối vào cổng quản lý trên router.

- Cổng console và cổng AUX là cổng quản lý trên router. Loại cổng nối tiếp bất đồng bộ này được thiết kế không phải để kết nối mạng mà là để cấu hình router. Ta thường sử dụng cổng console để thiết lập cấu hình cho router vì không phải router nào cũng có cổng AUX.

- Khi router hoạt động lần đầu tiên thì chưa có thông số mạng nào được cấu hình cả. Do đó router chưa thể giao tiếp với bất kỳ mạng nào. Để chuẩn bị khởi động và cấu hình router, ta dùng thiết bị đầu cuối ASCII kết nối vào cổng console trên router. Sau đó ta có thể dùng lệnh để cấu hình, cài đặt cho router.

- Khi nhập cấu hình cho router thông qua cổng console hay cổng AUX, router có thể kết nối mạng để xử lý sự cố hoặc theo dõi hoạt động mạng. Có thể cấu hình router từ xa bằng cách quay số qua modem kết nối vào cổng console hay cổng AUX trên router.

- Khi xử lý sự cố, nên sử dụng cổng console thay vì cổng AUX. Vì mặc định là cổng console có thể hiển thị quá trình khởi động router, thông tin hoạt động và các thông điệp báo lỗi của router. Cổng console được sử dụng khi có một dịch vụ mạng không khởi động được hoặc bị lỗi, khi khôi phục lại mật mã hoặc khi router bị sự cố nghiêm trọng.

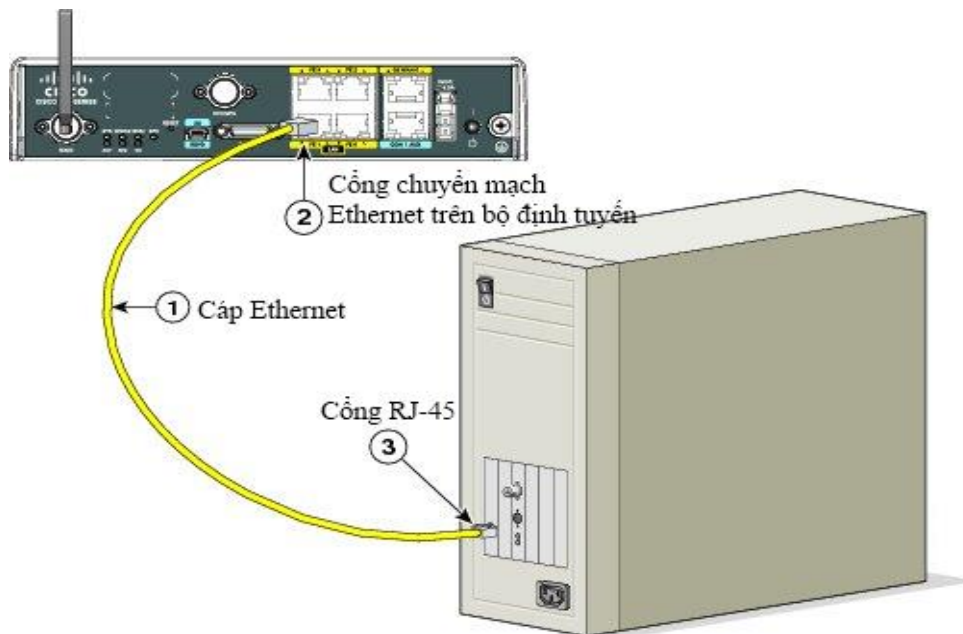
2.5 Thiết lập kết nối vào cổng console

- Cổng console là loại cổng quản lý, cung cấp đường kết nối riêng vào router. Cổng này được sử dụng để thiết lập cấu hình cho router, theo dõi hoạt động mạng và khôi phục router khi gặp sự cố nghiêm trọng.

- Để kết nối PC vào cổng console cần có cáp rollover và bộ chuyển đổi RJ45- DB9. Cisco có cung cấp bộ chuyển đổi này để nối PC vào cổng console.

- PC hay thiết bị đầu cuối phải có chương trình mô phỏng thiết bị đầu cuối VT100. Thông thường phần mềm này là HyperTerminal.

- Ta có mô hình như hình 1.12:



Hình 1. 12: Kết nối modem vào cổng console hay cổng AUX

- Chuẩn bị:
 - + Router
 - + PC
 - + Phần mềm HyperTerminal
 - + Cáp rollover
 - + Bộ chuyển đổi RJ45-DB9
- Các bước thực hiện:
 - ✓ **Bước 1:** Cấu hình phần mềm giả lập thiết bị đầu cuối như sau:
 - + Chọn đúng cổng COM.
 - + Tốc độ band là 9600.
 - + Data bits: 8.
 - + Parity: None.
 - + Stop bits: 1.
 - + Flow control: None
 - ✓ **Bước 2:** Cắm một đầu RJ45 của cáp rollover vào cổng console trên router.
 - ✓ **Bước 3:** Cắm đầu cáp còn lại vào bộ chuyển đổi RJ45-DB9.
 - ✓ **Bước 4:** Gắn đầu DB9 của bộ chuyển đổi vào cổng COM trên PC

3.BÀI TẬP THỰC HÀNH 1.1

3.1. Mô hình

Cho mô hình gồm PC kết nối với Router Cisco như hình 1.13:



Hình 1. 13: Mô hình PC kết nối với router

3.2.Yêu cầu:

- + Tải và cài đặt phần mềm Cisco Packet Tracer.
- + Kết nối Router vào PC qua cổng Console.
- + Cấu hình thiết bị đầu cuối với các thông số sau: 96000 baud, 8 data bits, 1 stop bit, no flow control.

3.3.Chuẩn bị:

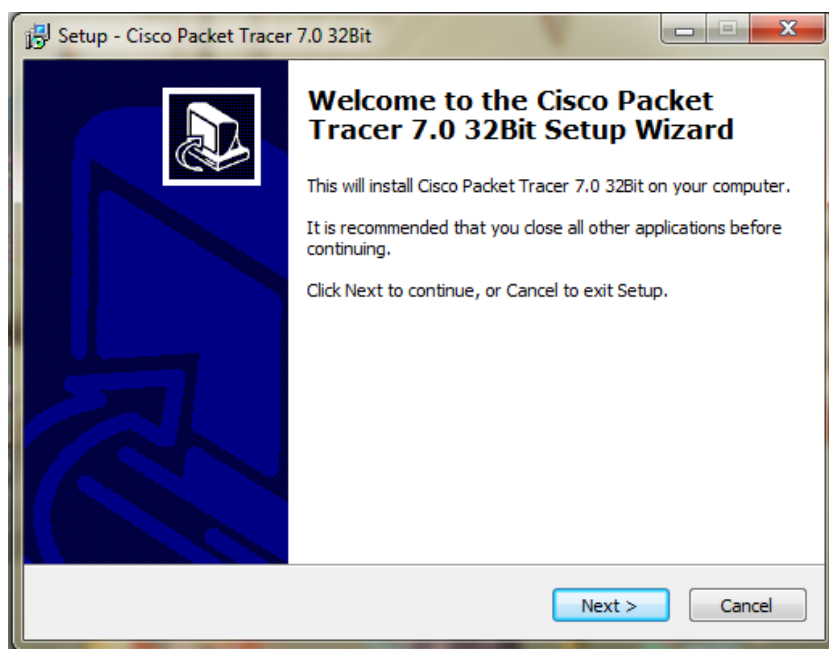
Bảng 1. 1:Chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 1.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	1	
3	Router ảo	Cái	1	

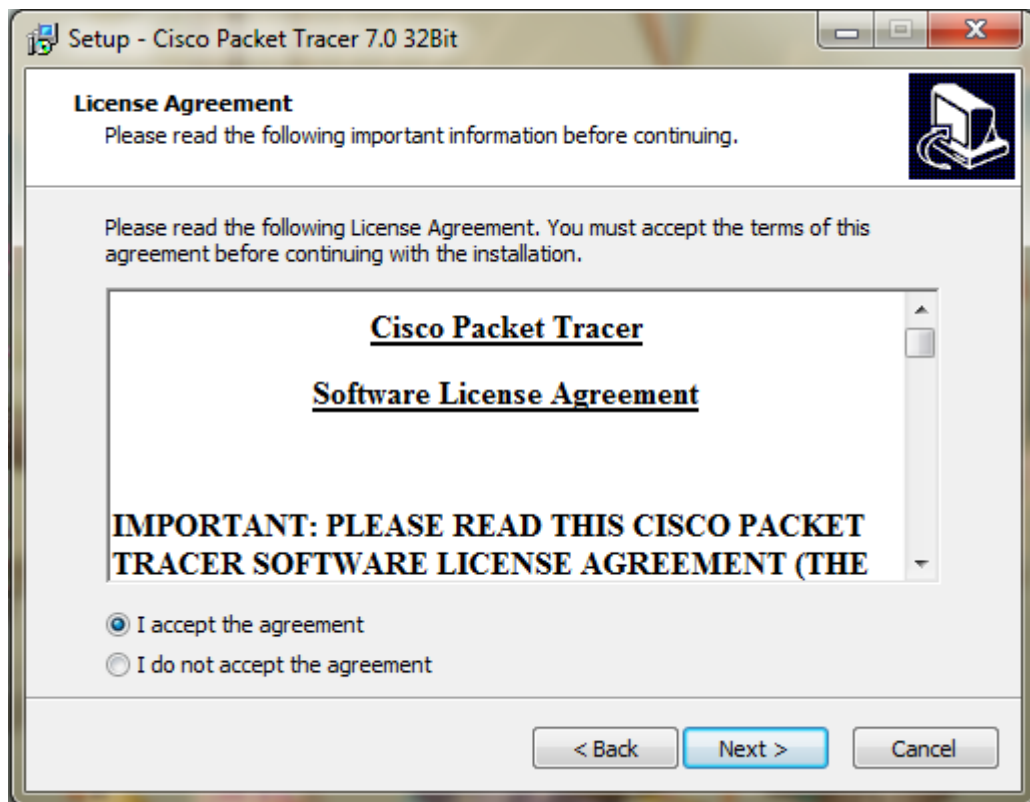
3.4.Các bước thực hành:

Bước 1: Tìm và tải phần mềm Cisco Packet Tracer trên các trang google.

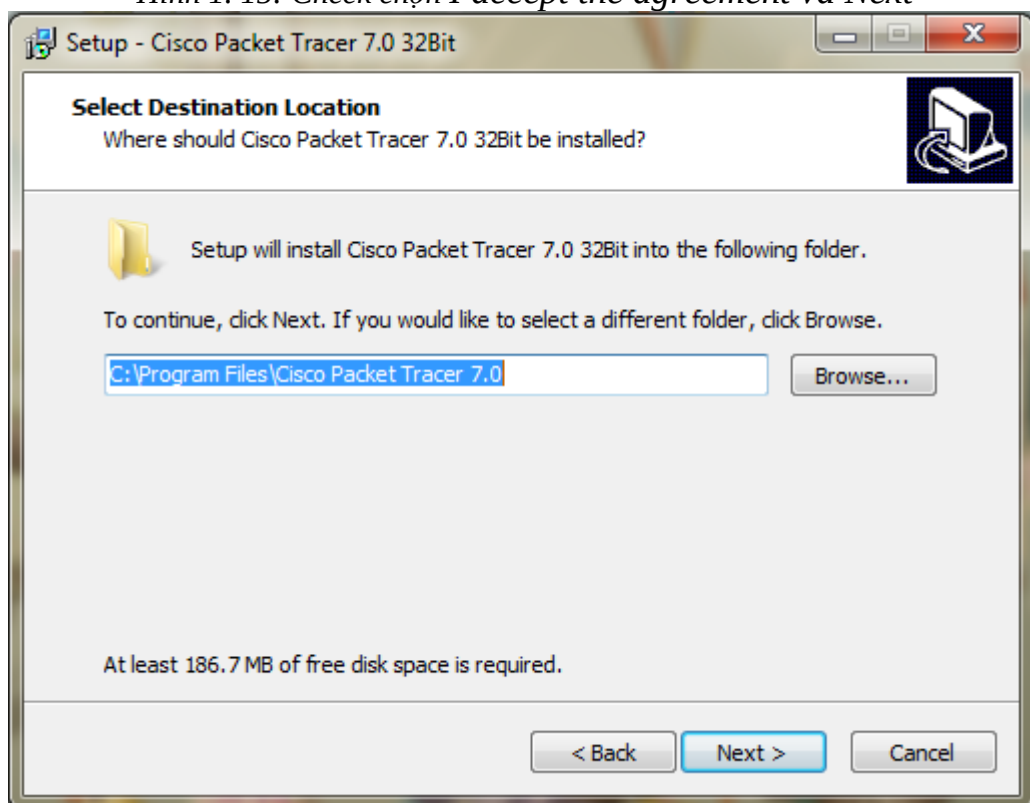
Bước 2: Cài đặt phần mềm:



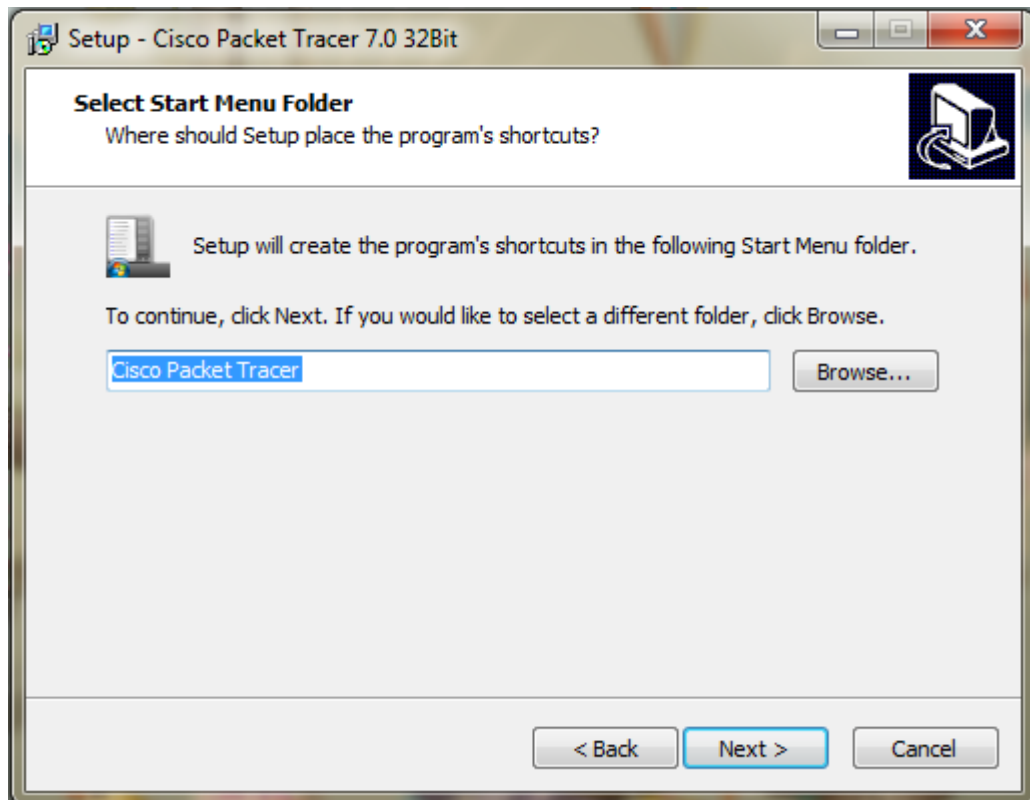
Hình 1. 14:Khởi động phần mềm



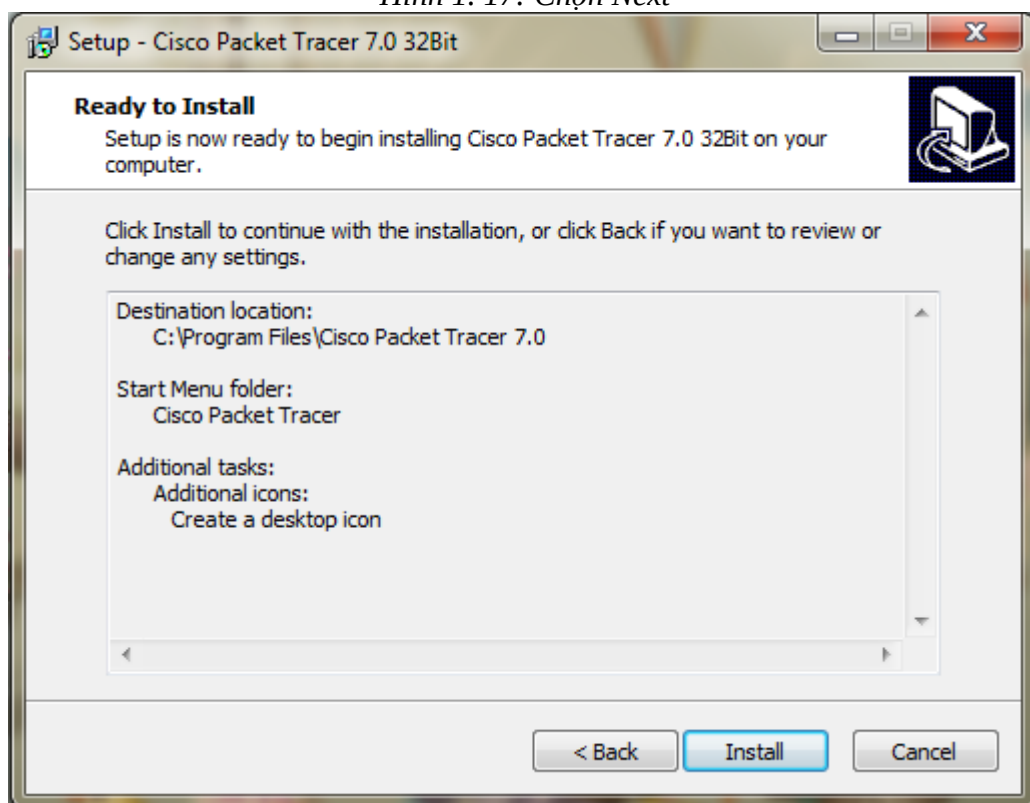
Hình 1. 15: Check chọn *I accept the agreement* và *Next*



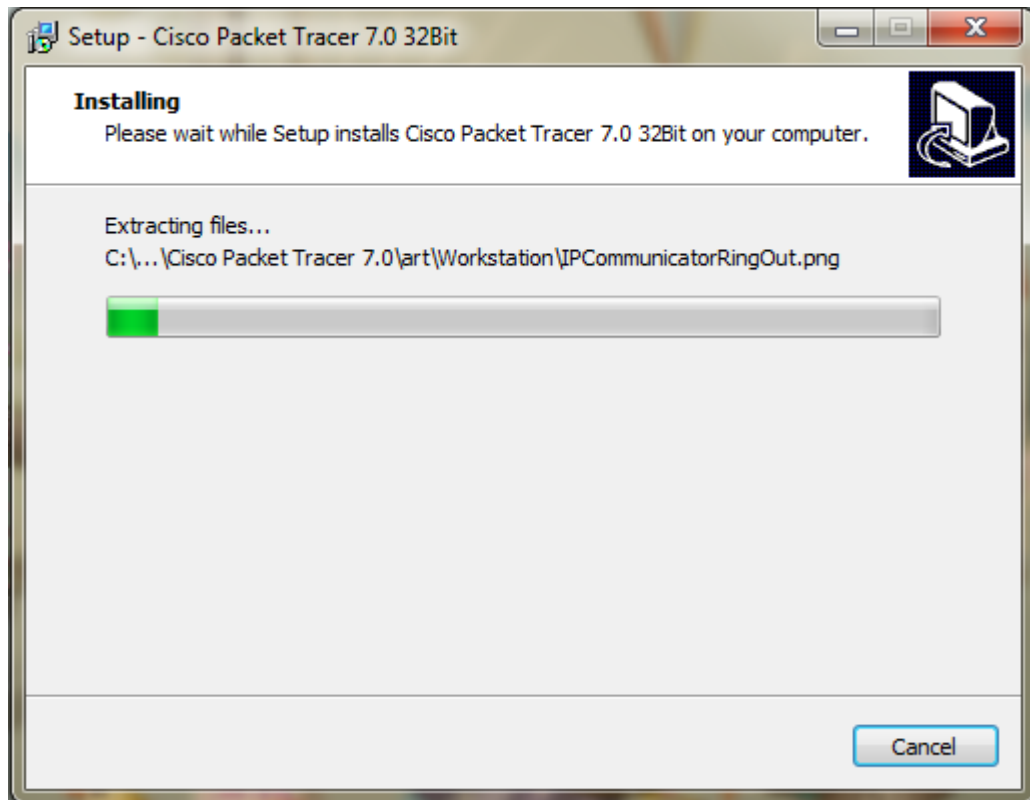
Hình 1. 16: Chọn vị trí lưu, nhấn *Browse...* nếu muốn thay đổi, sau đó chọn *Next* để tiếp tục



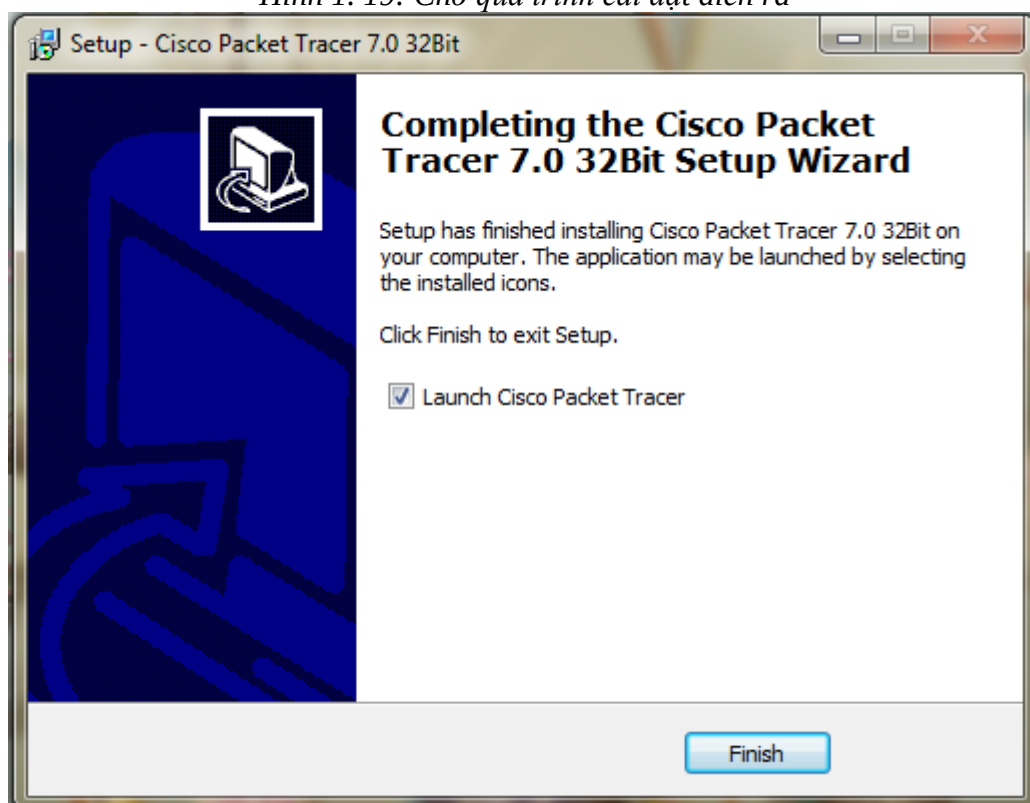
Hình 1. 17: Chọn Next



Hình 1. 18: Chọn install



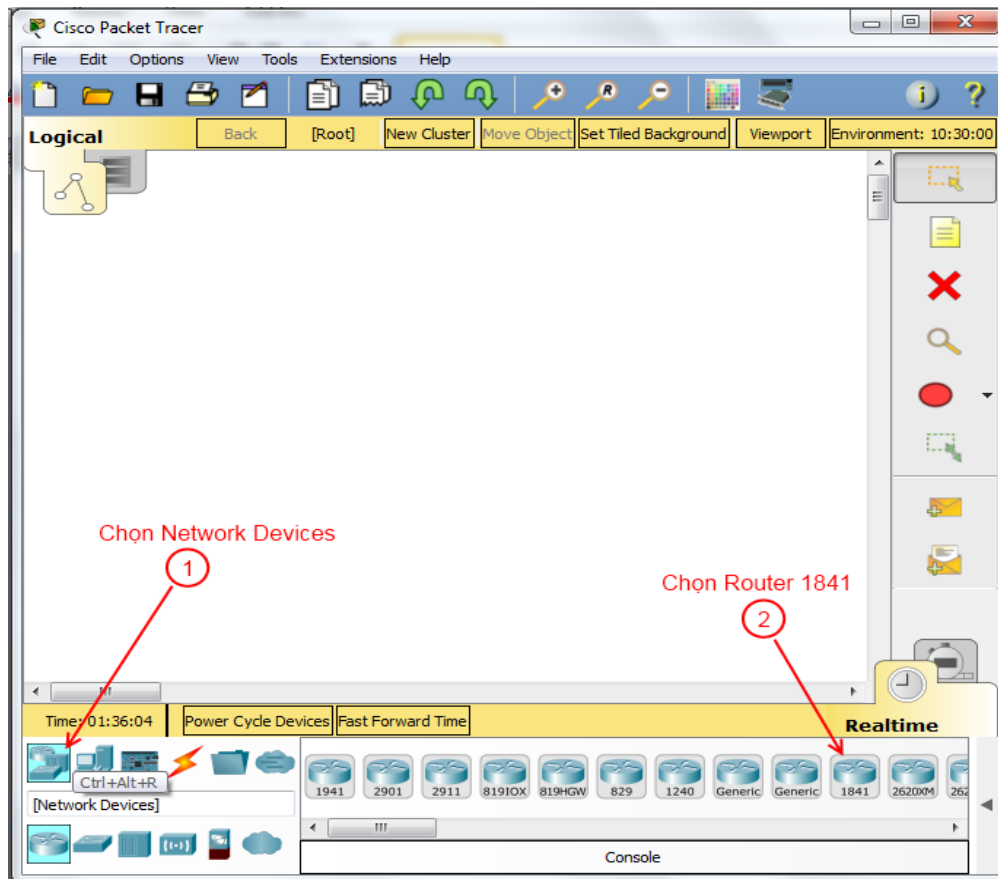
Hình 1. 19: Chờ quá trình cài đặt diễn ra



Hình 1. 20: Chọn finish

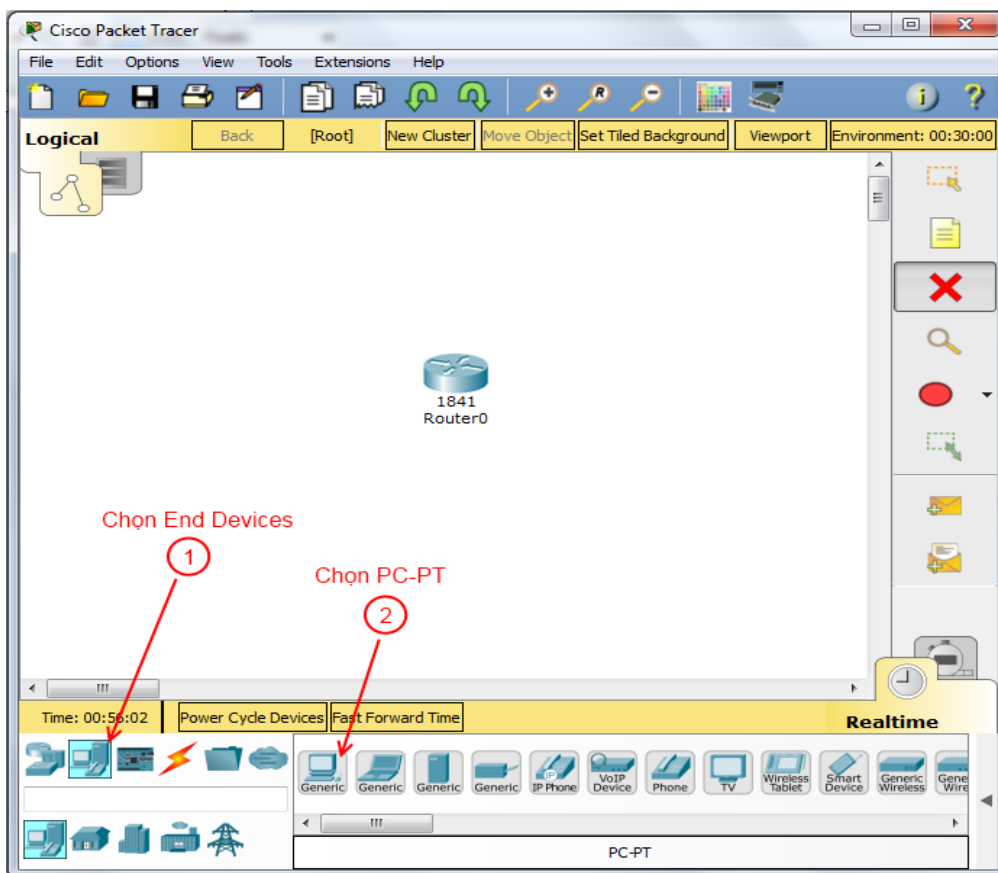
Bước 3: Xây dựng mô hình:

- Chọn Router: Phía dưới giao diện phần mềm, ta chọn [Network Devices]



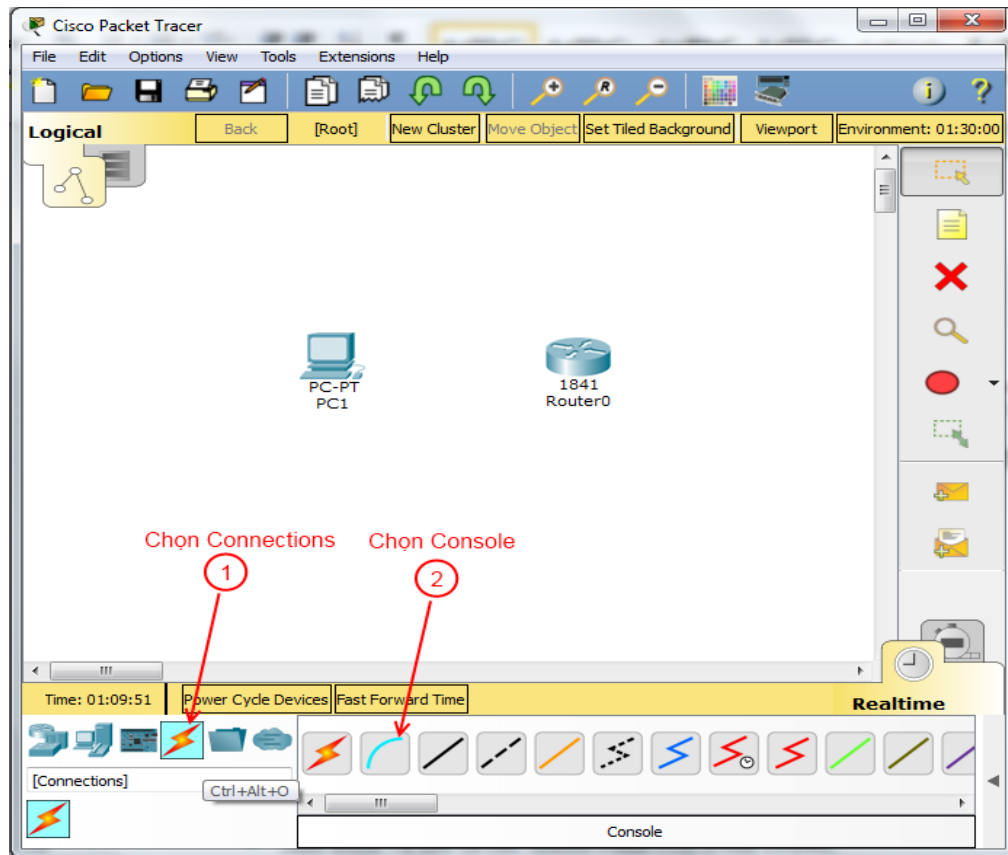
Hình 1. 21: Chọn Router 1841 và kéo ra giữa giao diện

- Chọn PC: Tương tự, ta chọn [End Devices]

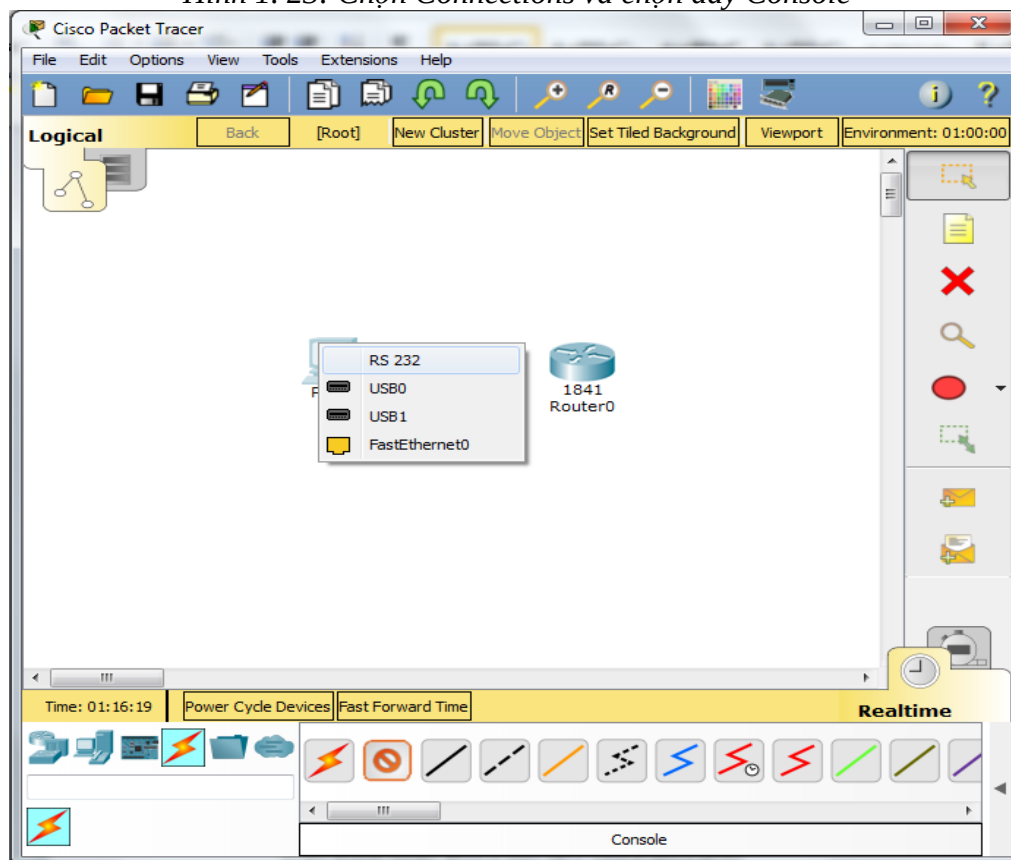


Hình 1. 22: Chọn PC-PT và kéo ra giữa giao diện

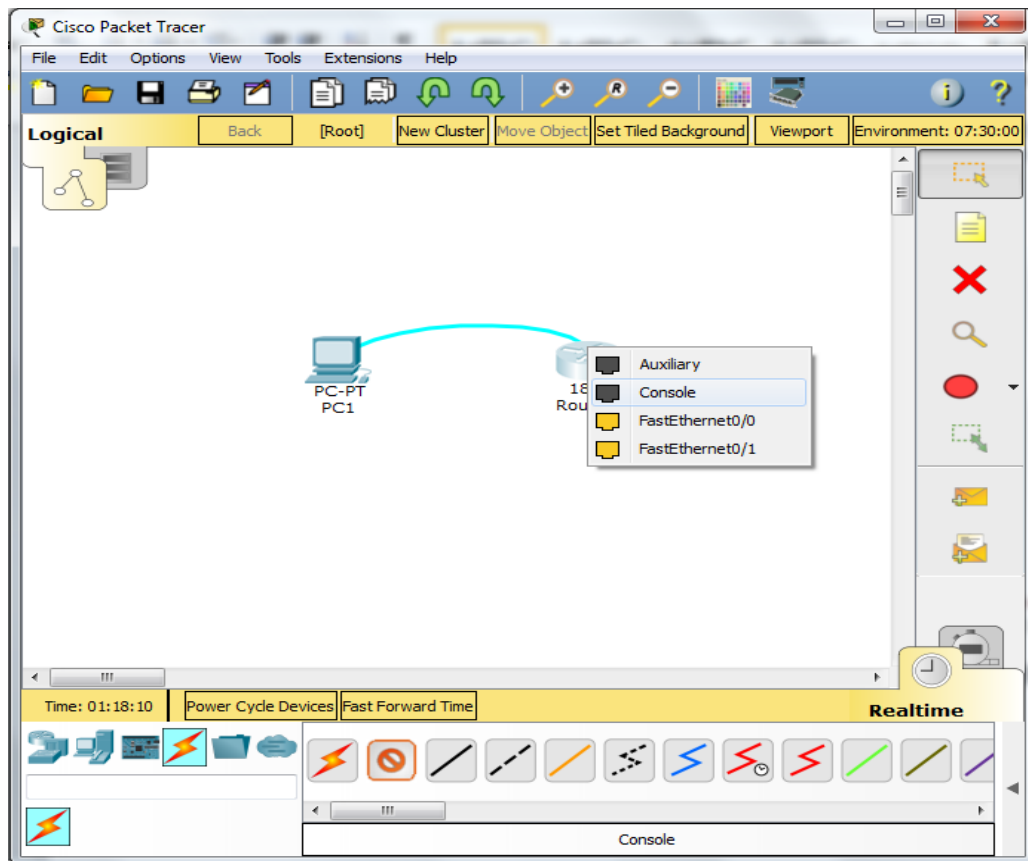
Bước 4: Kết nối PC với Router:



Hình 1. 23: Chọn Connections và chọn dây Console

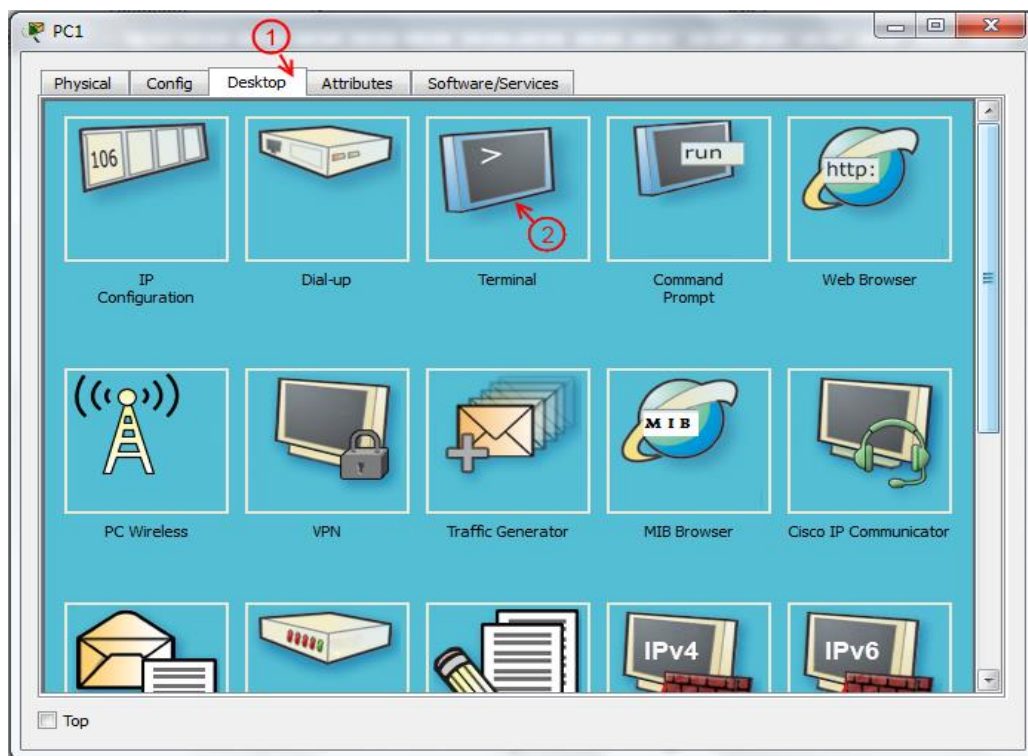


Hình 1. 24: Chọn đầu RS 232 với PC-PT

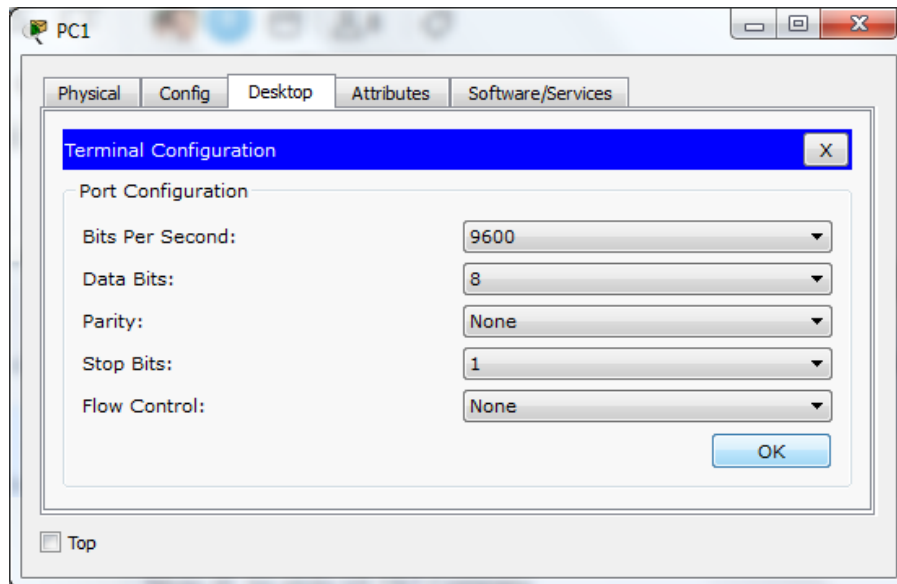


Hình 1. 25: Với Router ta chọn cổng Console

Bước 5: Cấu hình thiết bị đầu cuối với các thông số sau: 96000 baud, 8 data bits, 1 stop bit, no flow control.



Hình 1. 26: Nhấn vào PC, chọn Desktop sau đó chọn Terminal



Hình 1. 27: Chỉnh về các thông số sau: 96000 baud, 8 data bits, 1 stop bit, no flow control

3.5. Những sự cố thường gặp

Bảng 1. 2: những sự cố thường gặp của bài tập 1.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Máy tính chạy chậm	Thiếu dung lượng bộ nhớ RAM	Khi tạo máy ảo chia dung lượng bộ nhớ RAM tối thiểu 512MB
Phần mềm Cisco Packet Tracer thiếu chức năng	Do phiên bản Cisco Packet Tracer đã cũ	Cập nhật phiên bản mới
Không thông mạng	Do đặt sai địa chỉ IP	Kiểm tra và đặt lại địa chỉ IP
Ping thông mạng nhưng các thông số trên router không đúng	Do khi cài đặt chọn sai thông số	Kiểm tra đặt lại các thông số trên router

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7. Đánh giá các bước thực hành

Bảng 1. 3: đánh giá các bước thực hành bài tập 1.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Tìm và tải phần mềm Cisco Packet Tracer trên các trang google.	Tìm đúng địa chỉ			
2	Bước 2: Cài đặt phần mềm	Chọn đúng các mục			
3	Bước 3: Xây dựng mô hình	Chọn đúng thiết bị			
4	Bước 4: Kết nối PC với Router	Chọn đúng dây, đúng cổng			
5	Bước 5: Cấu hình thiết bị đầu cuối với các thông số sau: 96000 baud, 8 data bits, 1 stop bit, no flow control	Chọn đúng các thông số			

4.TÓM TẮT NỘI DUNG

- Khái niệm về WAN và LAN.
- Vai trò của router trong WANs và LANs.
- Các giao thức WAN.
- Cấu hình kiểu đóng gói cho cổng giao tiếp.
- Xác định và mô tả các thành phần bên trong router.
- Đặc điểm vật lý của router.
- Các loại cổng thường gặp trên router.
- Cách kết nối vào cổng console, cổng LAN và WAN.

5.CÂU HỎI VÀ BÀI TẬP

Câu hỏi:

Câu 1: Trình bày khái niệm và đặt điểm của mạng WAN ? Các thiết bị nào được sử dụng trong mạng WAN?

Câu 2: Nêu các thành phần bên trong của Router và đặt điểm vật lý của Router?

Bài Tập:

- Cho mô hình gồm PC kết nối với Router Cisco như hình:



- Thực hiện kết nối với cổng WAN cho 2 Router..
- Cho phép interface hoạt động để 2 Router kết nối được với nhau.

BÀI 2: GIỚI THIỆU VỀ ROUTER

Mã bài MD 28-02

Thời gian: 7 giờ

I. MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày được mục đích của IOS;
- Trình bày hoạt động cơ bản của IOS;
- Xác định được phương thức thiết lập phiên giao tiếp bằng dòng lệnh với router;
- Chuyển đổi giữa các chế độ cấu hình router;
- Thiết lập kết nối bằng HyperTerminal vào router;
- Truy cập vào router;
- Sử dụng tính năng trợ giúp trong giao tiếp bằng dòng lệnh;
- Thực hiện các thao tác an toàn với máy tính;

II. NỘI DUNG CHÍNH

1. Giới thiệu hệ điều hành IOS.

1.1 Mục đích của phần mềm IOS.

- Tương tự như máy tính, router và switch không thể hoạt động được nếu không có hệ điều hành. Cisco gọi hệ điều hành của mình là hệ điều hành mạng Cisco hay gọi tắt là Cisco IOS. Hệ điều hành được cài trên các Cisco router và Catalyst Switch. Cisco IOS cung cấp các dịch vụ mạng như sau:

- + Định tuyến và chuyển mạch.
- + Bảo đảm và bảo mật cho việc truy cập vào tài nguyên mạng.
- + Mở rộng hệ thống mạng.

1.2 Giao diện người dùng của router.

- Phần mềm Cisco sử dụng giao diện dòng lệnh (CLI – Command – line interface) cho môi trường console truyền thống. IOS là một kỹ thuật cơ bản, từ đó được phát triển cho nhiều dòng sản phẩm khác nhau của Cisco. Do đó hoạt động cụ thể của từng IOS sẽ rất khác nhau tùy theo từng loại thiết bị.

- Có nhiều cách khác nhau để truy cập vào giao diện CLI của router:
 - + Cách đầu tiên là kết nối trực tiếp từ máy tính hoặc thiết bị đầu cuối vào cổng console trên router.
 - + Cách thứ hai là sử dụng đường quay số qua modem hoặc kết nối null modem vào cổng AUX trên router. Cả hai cách trên đều không cần phải cấu hình trước cho router.
 - + Cách thứ ba là telnet vào router. Để thiết lập phiên telnet vào router

router thì trên router ít nhất phải có một cổng đã được cấu hình địa chỉ IP các đường vty đã được cấu hình cho phép truy cập và đặt mật mã.

1.3 Các chế độ cấu hình router.

- Giao diện dòng lệnh của Cisco sử dụng cấu trúc phân cấp. Cấu trúc này đòi hỏi muốn cấu hình cái gì thì phải vào chế độ tương ứng. Ví dụ: nếu muốn cấu hình cổng giao tiếp nào của router thì phải vào chế độ cấu hình cổng giao tiếp đó. Từ chế độ này tất cả các cấu hình được nhập vào chỉ có hiệu lực đối với cổng giao tiếp tương ứng mà thôi. Tương ứng với mỗi chế độ cấu hình có một dấu nhắc đặc trưng riêng và một tập lệnh riêng.

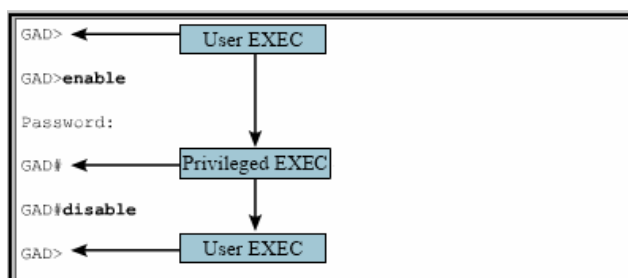
- IOS có một trình thông dịch gọi là EXEC. Sau khi nhập một câu lệnh thì EXEC sẽ thực thi ngay câu lệnh đó.

- Vì lý do bảo mật nên Cisco IOS chia phiên bản làm việc của EXEC thành hai chế độ là: chế độ EXEC người dùng và chế độ EXEC đặc quyền. Sau đây là các đặc điểm của chế độ EXEC người dùng và chế độ EXEC đặc quyền:

+ Chế độ EXEC người dùng chỉ cho phép thực thi một số câu lệnh hiển thị các thông tin cơ bản của router mà thôi. Chế độ này chỉ để xem chứ không cho phép thực hiện các câu lệnh làm thay đổi cấu hình router. Chế độ EXEC người dùng có dấu nhắc là “>”.

+ Chế độ EXEC đặc quyền cho phép thực hiện tất cả các câu lệnh của router. có thể cấu hình để người dùng phải nhập mật mã trước khi truy nhập vào chế độ này. Ngoài ra, để tăng thêm tính bảo mật có thể cấu hình thêm userID. Điều này cho phép chỉ những người nào được phép mới có thể truy cập vào router. Người quản trị mạng phải ở chế độ EXEC đặc quyền mới có thể sử dụng các câu lệnh để cấu hình hoặc quản lý router. Từ chế độ EXEC đặc quyền có thể chuyển vào các chế độ đặc khác nhau như chế độ cấu hình toàn cục chẳng hạn. Chế độ EXEC đặc quyền được xác định bởi dấu nhắc “#”.

- Để chuyển từ chế độ EXEC người dùng sang chế độ EXEC đặc quyền hạn dùng lệnh **enable** tại dấu nhắc “>”. Nếu mật mã đã được cài đặt thì router sẽ yêu cầu nhập mật mã. Vì lý do bảo mật nên các thiết bị mạng Cisco không hiển thị mật mã trong lúc nhập chúng. Sau khi mật mã được nhập vào chính xác thì dấu nhắc “>” chuyển thành “#” cho biết đang ở chế độ EXEC đặc quyền. gõ dấu chấm hỏi (?) ở dấu nhắc này thì sẽ thấy router hiển thị ra nhiều câu lệnh hơn so với ở chế độ EXEC người dùng.



Hình 2. 1: Các chế độ cấu hình Router

2. Các đặc điểm và hoạt động của phần mềm IOS

2.1 Các đặc điểm của phần mềm IOS

- Để tối ưu hoá phần mềm IOS cho nhiều loại thiết bị, Cisco đã phát triển nhiều loại phần mềm Cisco IOS. Mỗi loại phần mềm IOS phù hợp với từng loại thiết bị, với mức dung lượng bộ nhớ và với nhu cầu của khách hàng.

- Mặc dù có nhiều phần mềm IOS khác nhau cho nhiều loại thiết bị với nhiều đặc tính khác nhau nhưng cấu trúc lệnh cấu hình cơ bản thì vẫn giống nhau. Do đó kỹ năng cấu hình và xử lý sự cố có thể ứng dụng cho nhiều loại sản phẩm khác nhau.

- Tên của Cisco IOS được quy ước chia ra thành ba phần như sau:

- + Phần thứ nhất thể hiện loại thiết bị mà phần mềm IOS này có thể sử dụng được.
- + Phần thứ hai thể hiện các đặc tính của phần mềm IOS.
- + Phần thứ ba thể hiện nơi chạy phần mềm IOS trên router và cho biết phần mềm này được cung cấp dưới dạng nén hay không nén.

- có thể lựa chọn các đặc tính đặc biệt của IOS nhờ phần mềm Cisco Software Advisor. Cisco Software Advisor là một công cụ cung cấp các thông tin hiện tại và cho phép chọn lựa các đặc tính cho phù hợp với yêu cầu của hệ thống mạng.

Bảng 2. 1: Các đặt điểm của phần mềm IOS

The name has three parts, separated by dashes: e.g. xxx-	
• xxxx = Platform • yyyy = Feature • ww = Format – where It execute from if	
Name Codes	
Platform (Hardware) (Partial list)	
C1005	1005
C1600	1600
C1700	1700, 1720, 1750
C2500	25xx, 3xxx, 5100, AO (11.2 and later only)
C2600	2600
C2800	Catalyst 2800
C2900	2910, 2950
C3620	3620
C3640	3640
C4000	4000 (11.2 and later only)
C4500	4500, 4700
Feature (Partial list)	
B	Appletalk
Boot	Boot image

C	Commserver file (CiscoPro)
Drag	IOS based diagnostic images
G	ISDN subnet (SNMP, IP, Bridging, ISDN, PPP, IPX, Atalk)
I	IP subnet (SNMP, IP, Bridging, WAN, Remote Node, Terminal Services)
N	IPX
Q	Async
T	Telco return (12.0)
Y	Reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, ISDN, PPP) (C1003/4)
Z	Managed moderns
40	40 bit encryption
56	56 bit encryption
Format (Where the image runs in the route)	
F	Flash
M	Ram
R	Rom
L	Rebcatable
Compression Tyne	
Z	Zip compressed (note lower case)
X	M zip compressed
W	“STAC” compress

- Trước khi cài đặt phần mềm Cisco IOS mới lên router, phải kiểm tra xem router có đủ dung lượng bộ nhớ hay không. Để xem dung lượng RAM dùng lệnh **show version**:

...<output omitted>... PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

- Dòng trên cho biết dung lượng của bộ nhớ chính và bộ nhớ chia sẻ trên router. Có một số thiết bị sử dụng một phần DRAM làm bộ nhớ chia sẻ. Tổng hai dung lượng trên là dung lượng thật sự của DRAM trên router.

- Để xem dung lượng của bộ nhớ flash dùng lệnh **show flash**: GAD#**show flash**

...<output omitted>...

63488K bytes of processor board System flash (Read/Write)

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:pt1000-i-mz.122-28.bin"

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of
memory
-
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
--More--
```

Hình 2. 2: Lệnh show version

2.2 Hoạt động của phần mềm IOS

- Thiết bị Cisco IOS có 3 chế độ hoạt động sau:
 - + ROM monitor.
 - + Boot ROM.
 - + Cisco IOS.
- Thông thường trong quá trình khởi động router, một trong các chế độ hoạt động trên được tải lên RAM để chạy. Người quản trị hệ thống có thể cài đặt giá trị cho thanh ghi để điều khiển chế độ khởi động mặc định router.
- Chế độ ROM monitor thực hiện quá trình bootstrap và kiểm tra phần cứng. Chế độ này được sử dụng để khôi phục lại hệ thống khi bị lỗi nghiêm trọng hoặc khi người quản trị mạng bị mất mật mã. Chúng ta chỉ có thể truy cập vào chế độ ROM monitor bằng đường kết nối vật lý trực tiếp vào cổng console trên router. Ngoài ra chúng ta không thể truy cập vào chế độ này bằng bất kỳ cổng nào khác.
- Khi router ở chế độ boot ROM, chỉ có một phần chức năng của Cisco IOS là hoạt động được. Chế độ boot ROM cho phép chép được lên bộ nhớ flash, nên chế độ này thường được sử dụng để thay thế phần mềm Cisco IOS trong flash. Dùng lệnh **copy tftp flash** để chép phần mềm IOS trên TFTP server vào bộ nhớ flash trên router.

Operating Environment	Prompt	Usage
ROM monitor	> or ROMMON	Failure or password recovery
Boot ROM	Router (boot) >	Flash image upgrade
Cisco IOS	Router >	Normal operation

Hình 2. 3: 3 chế độ hoạt động

- Router muốn hoạt động bình thường thì phải chạt được toàn bộ phần mềm IOS trong flash. Ở một số thiết bị, phần mềm IOS được chạy trực tiếp từ flash. Tuy nhiên, hầu hết các Cisco router đều chép phần mềm IOS lên RAM rồi chạy từ RAM. Một số phần mềm IOS lưu trong flash dưới dạng nén và được giải nén khi chép lên RAM.

- dùng lệnh **show version** để xem các thông tin về phần mềm IOS, trong đó có hiển thị giá trị cấu hình của thanh ghi. Còn nếu muốn xem hệ thống còn bao nhiêu dung lượng bộ nhớ để tải phần mềm Cisco IOS mới thì dùng lệnh **show flash**.

```
Router>show flash

System flash directory:
File Length Name/status
  3 5571584 pt1000-i-mz.122-28.bin
  2 28282 sigdef-category.xml
  1 227537 sigdef-default.xml
[5827403 bytes used, 58188981 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Router>
```

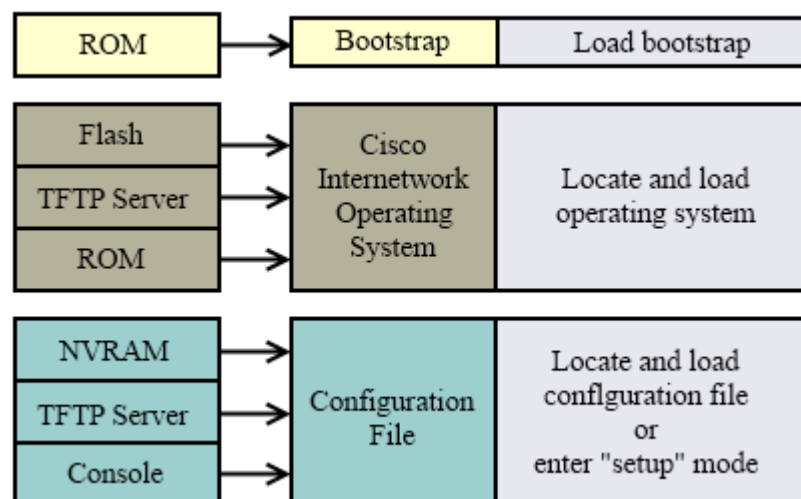
Hình 2. 4: Lệnh show flash

2.3 Khởi động router

- Router khởi động bằng cách tải bootstrap, hệ điều hành và tập tin cấu hình. Nếu router không tìm thấy tập tin cấu hình thì sẽ tự động vào chế độ cài đặt. Khi hoàn tất việc cấu hình trong chế độ cài đặt thì tập tin cấu hình đó sẽ được lưu trong NVRAM.

- Để cho router bắt đầu hoạt động, quá trình khởi động phần mềm Cisco IOS thực hiện 3 công đoạn sau:

- + Kiểm tra phần cứng của router và bảo đảm là chúng hoạt động tốt.
- + Tìm và tải phần mềm Cisco IOS.
- + Tìm và thực thi tập tin cấu hình khởi động hoặc vào chế độ cài đặt nếu không tìm thấy tập tin này.



Hình 2. 5: Các bước khởi động router

- Khi router mới được bật điện lên thì nó thực hiện quá trình tự kiểm tra POST (Power on self test). Trong quá trình này, router chạy một trình từ ROM để kiểm tra tất cả các thành phần phần cứng trên router, ví dụ như kiểm tra hoạt động của CPU, bộ nhớ và các cổng giao tiếp mạng. Sau khi hoàn tất quá trình này, router bắt đầu thực hiện khởi động phần mềm.

- Sau quá trình POST, router sẽ thực hiện các bước sau:

- **Bước 1:** Chạy chương trình nạp bootstrap từ ROM. Bootstrap chỉ đơn giản là một tập lệnh để thực hiện kiểm tra phần cứng và khởi động IOS.
- **Bước 2:** Tìm IOS. Giá trị khởi động trên thanh ghi cấu hình sẽ quyết định việc tìm IOS ở đâu. Nếu giá trị này cho biết là tải IOS từ flash hay từ mạng thì các câu lệnh boot system trong tập tin cấu hình sẽ cho biết chính xác vị trí và tên của IOS.
- **Bước 3:** Tải hệ điều hành đã được tải xuống và bắt đầu hoạt động thì các sẽ thấy hiện trên màn hình console danh sách các thành phần phần cứng và phần mềm có trên router.
- **Bước 4:** Tập tin cấu hình lưu trong VNVRAM được chép lên bộ nhớ chính và được thực thi từng dòng lệnh một. Các câu lệnh cấu hình thực hiện khởi động quá trình định tuyến, đặt địa chỉ cho các cổng giao tiếp mạng và thiết lập nhiều đặc tính hoạt động khác cho router.
- **Bước 5:** Nếu không tìm thấy tập tin cấu hình trong VNVRAM thì hệ điều hành sẽ đi tìm TFTP server. Nếu cũng không tìm thấy một TFTP server nào thì chế độ cài đặt sẽ được khởi động.

- Trong chế độ cài đặt, các không thể cấu hình cho các giao thức phức tạp của router. Mục đích của chế độ cài đặt chỉ là cho phép người quản trị mạng cài đặt một cấu hình tối thiểu cho router khi không thể tìm được tập tin cấu hình từ những nguồn khác.

- Trong chế độ cài đặt, câu trả lời mặc định được đặt trong dấu ngoặc vuông [] ở sau mỗi câu hỏi. Có thể nhấn phím Ctrl-C bất kỳ lúc nào để kết thúc quá trình cài đặt. Khi đó tất cả các cổng giao tiếp mạng trên router sẽ đóng lại.

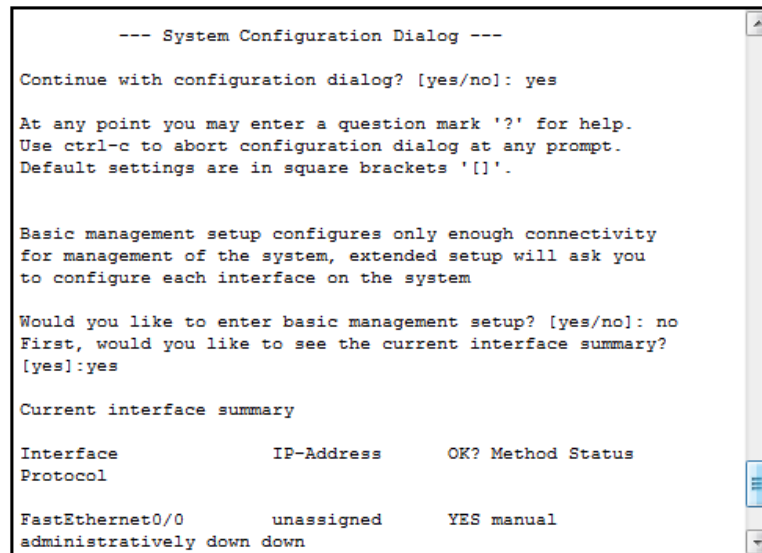
- Khi hoàn tất cấu hình trong chế độ cài đặt, sẽ gặp các dòng thông báo như sau:

[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:



Hình 2. 6: Chế độ cài đặt của router

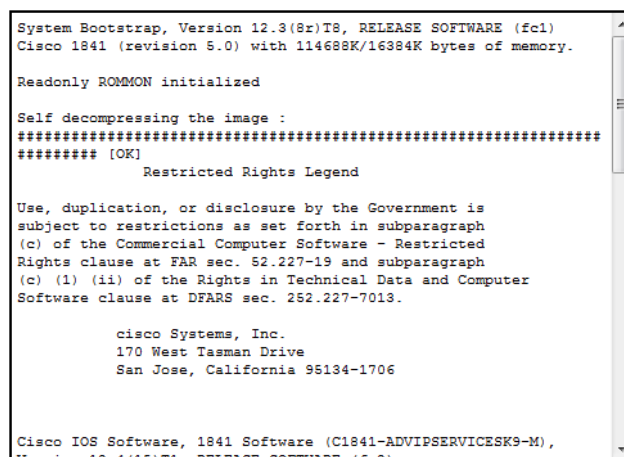
2.4 Đèn LED báo hiệu trên router.



Hình 2. 7: Báo hiệu đèn LED

- Cisco router sử dụng đèn LED để báo hiệu các trạng thái hoạt động của router. Các loại đèn LED này sẽ khác nhau tùy theo các loại router khác nhau.
- Các đèn LED của các cổng trên router sẽ cho biết trạng thái hoạt động của các cổng. Nếu đèn LED của một cổng nào đó bị tắt trong khi cổng đó đang hoạt động và được kết nối đúng thì chứng tỏ là đã có sự cố đối với cổng đó.
- Nếu một cổng hoạt động liên tục thì đèn LED của cổng đó sáng liên tục. Còn đèn LED OK ở bên phải cổng AUX sẽ bật sáng sau khi router hoạt động tốt.

2.5 Khảo sát quá trình khởi động router.



Hình 2. 8: Thông tin hiển thị trong quá trình khởi động router

- Ví dụ ở hình 2.8 cho thấy nội dung các thông điệp được hiển thị trên màn hình console trong suốt quá trình khởi động của router.
- Các thông tin này sẽ khác nhau tùy theo các loại cổng có trên router và tùy theo từng phiên bản Cisco IOS.

```

msb0 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: |

```

Hình 2. 9: Chế độ cấu hình

- Thông thường khi router đã được cấu hình thì tập tin cấu hình được lưu trong NVRAM, sau đó ta phải cấu hình thanh ghi để router sử dụng tập tin cấu hình này. Giá trị mặc định của thanh ghi cấu hình là 0x2102, khi đó router sẽ khởi động với Cisco IOS tải từ bộ nhớ flash và tập tin cấu hình tải từ NVRAM.

```

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE
SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K
bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

```

Hình 2. 10: Hiển thị thông tin phiên bản của bootstrap và IOS

- Theo hình 2.11 chúng ta có thể xác định được phiên bản của phần mềm bootstrap và IOS đang được sử dụng trên router. Ngoài ra cũng xác định được phiên bản của router, bộ xử lý là loại gì, dung lượng của bộ nhớ và một số các thông tin khác của router như:

- + Số lượng các cổng giao tiếp.
- + Các loại cổng giao tiếp.
- + Dung lượng NVRAM.
- + Dung lượng bộ nhớ flash.

2.6 Thiết lập phiên kết nối bằng HyperTerminal.

- Tất cả các Cisco router đều có cổng console nối tiếp bất đồng bộ TIA/EIA-232 (RJ45). Chúng ta cần phải có cáp và bộ chuyển đổi để kết nối từ thiết bị đầu cuối console vào cổng console trên router. Thiết bị đầu cuối console có thể là một thiết bị đầu cuối ASCII hoặc là một PC có chạy chương trình mô phỏng HyperTerminal. Để kết nối PC có cổng console chúng ta dùng cáp rollover và bộ chuyển đổi RJ45- DB9.

- Thông số mặc định của cổng console là: 9000 baud, 8 data bits, 1 stop bit, no flow control. Cổng console không có hỗ trợ điều khiển luồng bằng phần cứng. Sau đây là bước thực hiện để kết nối một thiết bị đầu cuối vào cổng console trên router.

- + Kết nối thiết bị đầu cuối vào cổng console trên router bằng cáp rollover và bộ chuyển đổi RJ45-DB9 hoặc RJ45-DB25.
- + Cấu hình thiết bị đầu cuối hoặc cấu hình phần mềm mô phỏng trên PC với các thông số sau: 9600 baud, 8 data bits, 1 stop bit, no flow control.

2.7 Truy cập vào router.

- Để cấu hình router phải truy cập vào giao diện người dùng của router bằng thiết bị đầu cuối hoặc bằng đường truy cập từ xa. Sau khi truy cập được vào router thì mới có thể nhập các câu lệnh cho router .

- Vì lý do bảo mật nên router có 2 mức truy cập:

- + Mức EXEC người dùng: chỉ có một số câu lệnh dùng để xem trạng thái của router. Ở mức này, không thể thay đổi được cấu hình của router.
- + Mức EXEC đặc quyền: bao gồm tất cả các câu lệnh để cấu hình router.

- Ngay sau khi truy cập được vào router sẽ gặp dấu nhắc của chế độ EXEC người dùng. Để sử dụng được toàn bộ tập lệnh phải chuyển vào chế độ EXEC đặc quyền. Ở dấu nhắc “>” gõ lệnh **enable**. Ở dấu nhắc **password:** phải nhập mật mã đúng với mật mã đã được cấu hình cho router trước đó bằng lệnh **enable secret** hoặc **enable password**. Nếu mật mã của router đã được cấu hình bởi cả 2 lệnh trên thì mật mã của câu lệnh **enable secret** sẽ được áp dụng. Sau khi hoàn tất các bước trên sẽ gặp dấu nhắc “#” cho biết là đang ở chế độ EXEC đặc quyền. Từ chế độ này mới có thể truy cập vào chế độ cấu hình toàn cục rồi sau đó là các chế độ cấu hình riêng biệt hơn như:

- + Chế độ cấu hình cổng giao tiếp.
- + Chế độ cấu hình cổng giao tiếp con.

- + Chế độ cấu hình đường truy cập.
- + Chế độ cấu hình router.
- + Chế độ cấu hình route-map.
- Từ chế độ EXEC đặc quyền, gõ disable hoặc exit để trở về chế độ EXEC người dùng. Để trở về chế độ EXEC đặc quyền từ chế độ cấu hình toàn cục, dùng lệnh exit hoặc Ctrl-Z. Lệnh Ctrl-Z có thể sử dụng để trở về ngay chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.

```
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router> ←————— User-Mode Prompt
Router>enable
Password:
Router# ←————— Privileged-Mode Prompt
Router#disable
Router>
Router>exit
```

Hình 2. 11: Chế độ EXEC đặc quyền

2.8 Phím trợ giúp trong router CLI

- Khi gõ dấu chấm hỏi (?) ở dấu nhắc thì router sẽ hiển thị danh sách các lệnh tương ứng với chế độ cấu hình mà đang ở. Chữ “--More--” ở cuối màn hình cho biết là phần hiển thị vẫn còn tiếp. Để xem trang tiếp theo, nhấn nhanh Spacebar. Còn nếu muốn hiển thị tiếp từng dòng một thì nhấn phím Enter hoặc Return. Có thể nhấn từng dòng một thì nhấn phím bất kỳ nào khác để quay trở về dấu nhắc.

```
Router>enable
Router#?
Exec commands:
<1-99>      Session number to resume
auto        Exec level Automation
clear       Reset functions
clock       Manage the system clock
configure   Enter configuration mode
connect     Open a terminal connection
copy        Copy from one file to another
debug       Debugging functions (see also 'undebug')
delete      Delete a file
dir         List files on a filesystem
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
erase       Erase a filesystem
exit        Exit from the EXEC
logout      Exit from the EXEC
mkdir       Create new directory
more        Display the contents of a file
no          Disable debugging informations
ping        Send echo messages
reload      Halt and perform a cold restart
--More--
```

Hình 2. 12: Danh sách lệnh sử dụng ở chế độ EXEC đặt quyền

- Để chuyển vào chế độ EXEC đặc quyền gõ **enable** hoặc gõ tắt là **ena** cũng được. Nếu mật mã đã được cài đặt vào cho router thì router sẽ yêu cầu

nhập mật mã. Sau khi đã vào được chế độ này rồi thì gõ dấu chấm hỏi (?), sẽ thấy là danh sách các câu lệnh dùng cho chế độ EXEC đặc quyền nhiều hơn hẳn danh sách các câu lệnh mà thấy trong chế độ EXEC người dùng. Tuy nhiên các tập lệnh này sẽ khác nhau tùy theo cấu hình của router và tùy theo từng phiên bản phần mềm Cisco IOS.

- Giả sử muốn cài đặt đồng hồ cho router nhưng lại không biết phải dùng lệnh nào thì khi đó chức năng trợ giúp của router sẽ giúp tìm được câu lệnh đúng. Thực hiện theo các bước sau:

➤ **Bước 1:** Dùng dấu chấm hỏi để tìm câu lệnh cài đặt đồng hồ. Trong danh sách các câu lệnh được hiển thị sẽ tìm được lệnh **clock**.

➤ **Bước 2:** Kiểm tra cú pháp câu lệnh để khai báo giờ.

➤ **Bước 3:** nhập giờ, phút, giây theo đúng cú pháp câu lệnh. sẽ gặp câu thông báo là câu lệnh chưa hoàn tất.

➤ **Bước 4:** nhấn **Ctrl-P** hoặc phím mũi tên (↑) để lại lệnh vừa mới nhập. Ở cuối câu lệnh đó thêm một khoảng trắng và dấu chấm hỏi (?) để xem phần kế tiếp của câu lệnh. Sau đó nhập lại đầy đủ câu lệnh.

➤ **Bước 5:** Nếu gặp dấu (^) thì có nghĩa là câu lệnh đã bị nhập sai. Vị trí của dấu (^) sẽ cho biết vị trí mà câu lệnh từ đâu cho tới vị trí mà dấu (^) chỉ sai rồi sẽ nhập thêm dấu chấm hỏi (?) để thêm cú pháp đúng tiếp theo của câu lệnh.

➤ **Bước 6:** nhập lại đầy đủ câu lệnh theo đúng cú pháp rồi nhấn phím **Enter** hoặc **Return** để thực thi câu lệnh.

2.9 Mở rộng thêm về cách viết câu lệnh

- Trong giao diện người dùng của router, router có thể có chế độ hỗ trợ soạn thảo câu lệnh. có thể sử dụng các tổ hợp phím như hình 2.14 để di chuyển con trỏ trên dòng lệnh mà đang viết khi cần phải chỉnh sửa câu lệnh đó. Trong các phiên bản phần mềm hiện nay, chế độ hỗ trợ soạn thảo câu lệnh là hoàn toàn tự động. Tuy nhiên nếu chế độ này làm ảnh hưởng các script thì có thể tắt bằng lệnh **terminal no editing** trong chế độ EXEC đặc quyền.

Bảng 2. 2: tổ hợp phím

Command	Description
Ctrl-A	Moves to the beginning of the command
Esc-B	Moves back one word
Ctrl-B (or right arrow)	Moves back one character
Ctrl-E	Moves to the end of the command line
Ctrl-F (or left arrow)	Moves forward one character
Esc-F	Moves forward one word

- Khi soạn thảo câu lệnh, màn hình sẽ cuộn ngang khi câu lệnh dài quá một hàng. Khi con trỏ đến hết lề phải thì dòng lệnh sẽ dịch sang trái 10 khoảng trắng. Khi đó 10 ký tự đầu tiên của câu lệnh sẽ không nhìn thấy được trên màn hình nữa. có thể cuộn lại để xem bằng cách nhấn **Ctrl-B** hoặc nhấn

phím mũi tên (←) cho tới khi màn hình cuộn tới đầu câu lệnh. Hoặc có thể nhấn **Ctrl-A** để chuyển ngay về đầu dòng lệnh.

- Ví dụ khi một câu lệnh dài quá một hàng. Dấu (\$) cho biết là câu lệnh đã được dịch sang trái. Phím **Ctrl-Z** được sử dụng để quay trở về chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.

2.10 Gọi lại các lệnh đã sử dụng

- Khi cấu hình router, router có lưu lại một số các lệnh đã sử dụng. Điều này đặc biệt có ích khi muốn lặp lại các câu lệnh dài và phức tạp. Với cơ chế này có thể thực hiện các việc sau:

- Cài đặt kích thước vùng bộ đệm để lưu các câu lệnh đã sử dụng.
- Gọi lại các câu lệnh đã sử dụng.
- Tắt chức năng này đi.

- Mặc định là router sẽ lưu lại 10 câu lệnh trong bộ đệm. Có thể thay đổi số lượng câu hỏi mà router lưu lại bằng lệnh **terminal history size** hoặc **history size**. Tối đa là 255 câu lệnh có thể lưu lại được.

- Nếu muốn gọi lại câu lệnh vừa mới sử dụng gần nhất thì nhấn **Ctrl-P** hoặc phím mũi tên (↑). Nếu tiếp tục nhấn thì mỗi lần nhấn như vậy sẽ gọi lại tuần tự các câu lệnh trước đó nữa. Nếu muốn gọi lại một câu lệnh sau đó thì nhấn **Ctrl-N** hoặc nhấn phím mũi tên (↓). Tương tự, nếu tiếp tục nhấn như vậy thì mỗi lần nhấn sẽ gọi lại một lệnh đó.

- Khi gõ lệnh, chỉ cần gõ các ký tự đủ để router phân biệt với mọi câu lệnh khác rồi nhấn phím **Tab** thì router sẽ tự động hoàn tất câu lệnh cho. Khi dùng phím **Tab** mà router hiển thị được đủ câu lệnh thì có nghĩa là router đã nhận biết được câu lệnh mà muốn nhập.

- Ngoài ra, hầu hết các router đều có thêm chức năng cho đánh dấu khối và copy. Nhờ đó có thể copy câu lệnh trước đó rồi dán hoặc chèn vào câu lệnh hiện tại.

Bảng 2. 3: Giải thích lệnh

Lệnh	Giải thích lệnh
Ctrl-P or up arrow key	Gọi lại lệnh ngay trước đó
Ctrl-N or down arrow key	Gọi lại lệnh ngay sau đó
Router> show history	Xem các lệnh đã sử dụng còn lưu trong bộ đệm
Router> Terminal history size number-of-lines	Cài đặt dung lượng bộ đệm đã lưu các lệnh đã sử dụng
Router> terminal no editing	Tắt chức năng soạn thảo lệnh nâng
Router> terminal editing	Mở chức năng soạn thảo lệnh nâng
< Tab >	Hoàn tất câu lệnh

2.11 Xử lý lỗi câu lệnh

- Lỗi câu lệnh thường là do gõ sai. Sau khi gõ một câu lệnh bị sai thì sẽ

gặp dấu báo lỗi (^). Dấu báo lỗi (^) đặt ở vị trí mà câu lệnh bắt đầu bị sai. Dựa vào đó và vận dụng chức năng trợ giúp của hệ thống sẽ tìm ra và chỉnh sửa lại lỗi cú pháp của câu lệnh.

Router#**clock set 13:32:00 February 93**

% Invalid input detected at “^” marker

- Trong ví dụ trên, dấu báo lỗi cho biết câu lệnh bị sai ở số 93. Gõ lại câu lệnh từ đầu tới vị trí bị lỗi rồi thêm dấu chấm hỏi (?) như sau:

Router # **clock set 13:32:00 February ?**

<1993-2035>Year

- Sau đó nhập lại câu lệnh với số năm đúng như cú pháp ở trên:

Router#**clock set 13:32:00 February 1993**

- Sau khi gõ xong câu lệnh rồi nhấn phím Enter mà câu lệnh đó bị sai thì có thể dùng phím mũi tên (↑) để gọi câu lệnh vừa mới nhập. Sau đó dùng các phím mũi tên sang phải, sang trái di chuyển con trỏ tới vị trí bị sai để sửa lại. Nếu cần xoá các ký tự thì có thể dùng phím <backspace>.

2.12 Lệnh show version

- Lệnh show version dùng để hiển thị các thông tin về phiên bản phần mềm Cisco IOS đang chạy trên router, trong đó có cả thông tin về giá trị thanh ghi cấu hình.

- Thông tin được hiển thị do lệnh show version bao gồm:

- Phiên bản IOS và một ít thông tin đặc trưng.
- Phiên bản phần mềm Bootstrap ROM.
- Phiên bản phần mềm Boot ROM.
- Thời gian hoạt động của router.
- Phương thức khởi động router lần gần đây nhất.
- Tên và vị trí lưu phần mềm hệ điều hành.
- Phiên bản phần cứng của router.
- Giá trị cài đặt của thanh ghi cấu hình.

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE
(fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:pt1000-i-mz.122-28.bin"

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of
memory
-
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
--More--
```

Hình 2. 13: Hiển thị do lệnh show version

- Chúng ta thường sử dụng lệnh show version để xác định phiên bản của phần mềm IOS và xem giá trị thanh ghi cài đặt cho quá trình khởi động của router.

3.BÀI TẬP THỰC HÀNH 2.1

3.1.Mô hình

Cho mô hình đơn giản gồm 1 PC kết nối với Router Cisco như hình 2.17:



Hình 2. 14: Mô hình PC kết nối Router

3.2. Yêu cầu

- + Khởi động router và thực hiện các bước cài đặt cơ bản trên router.
- + Cài đặt đồng hồ cho router.
- + Sử dụng lệnh **Show version** để xem thông tin về phần mềm Cisco IOS đang chạy trên Router.
- + Sử dụng lệnh **Show flash** để kiểm tra dung lượng bộ nhớ của Router.

3.3. Chuẩn bị

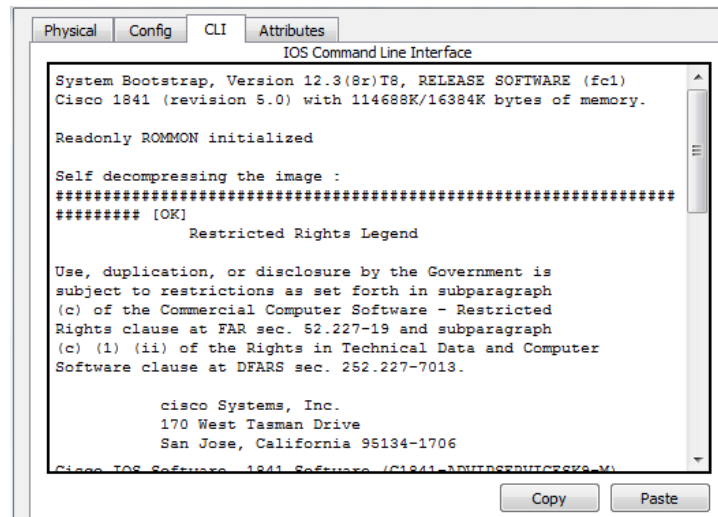
Bảng 2. 4: Chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 2.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	1	
3	Router ảo	Cái	1	

3.4. Các bước thực hành:

Bước 1: Khởi động router:

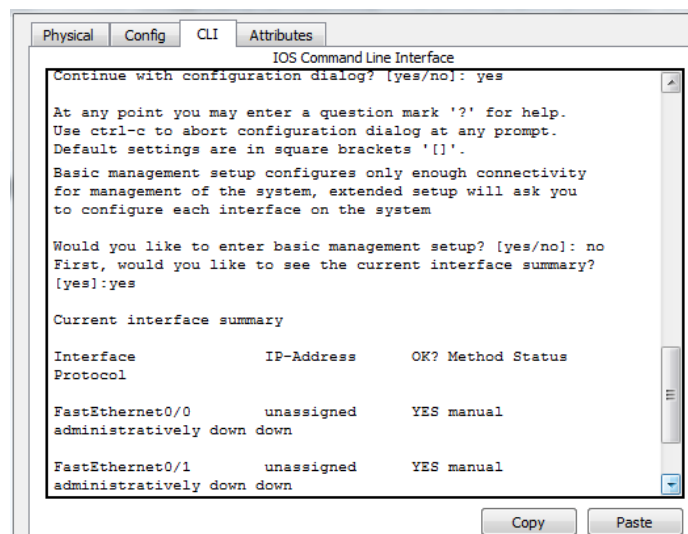
- Để khởi động router ta nhấn vào router đã chọn, sau đó chọn CLI



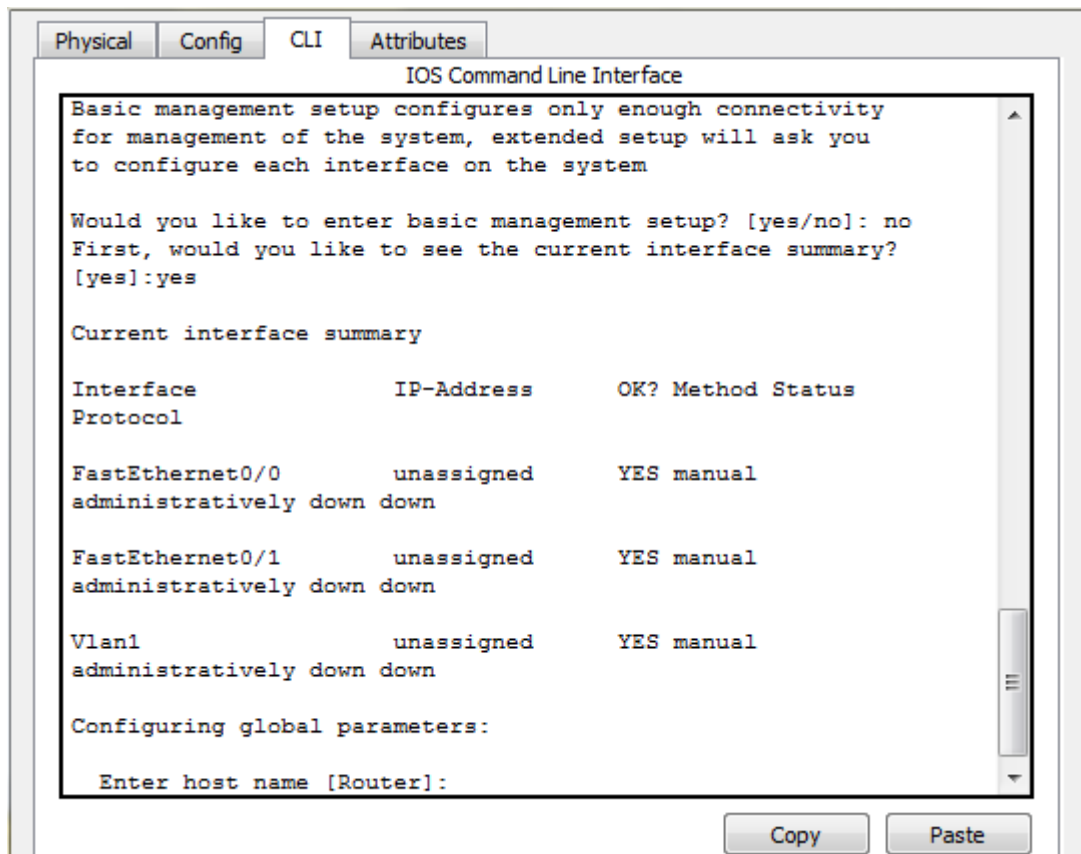
Hình 2. 15: Chọn CLI sẽ thấy thông tin quá trình khởi động router

Bước 2: Cài đặt cấu hình cơ bản trên Router:

- Tại dòng *Continue with configuration dialog? [yes/no]* ta nhập Yes

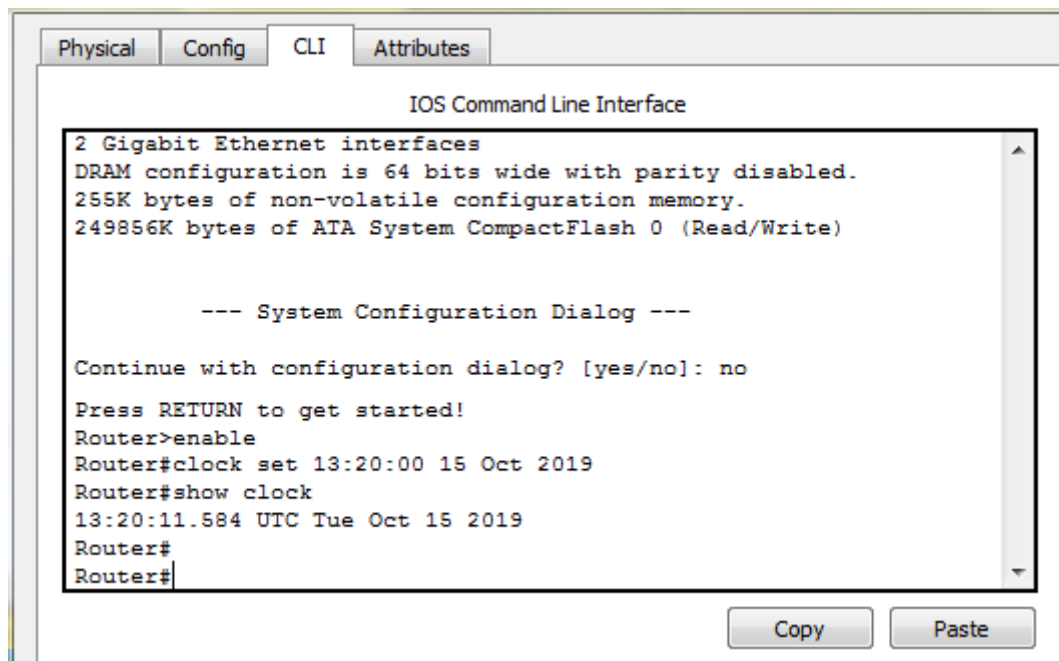


Hình 2. 16: Chế độ cấu hình router



Hình 2. 17: cấu hình cho Router

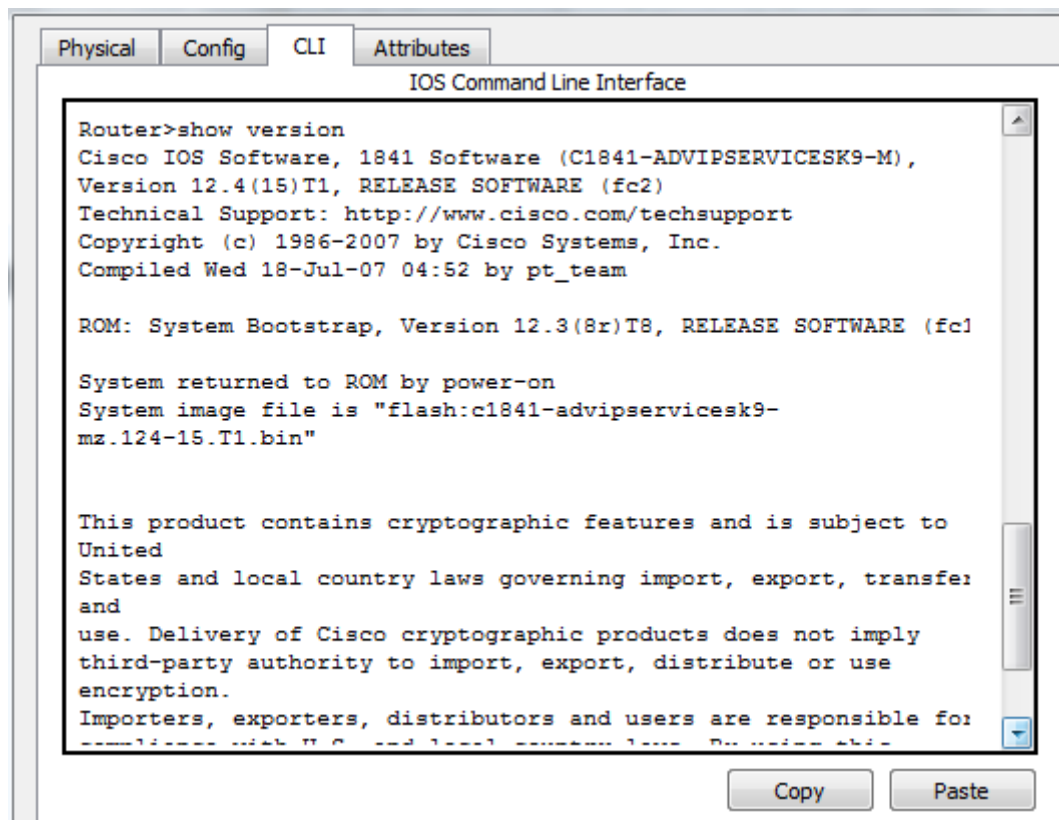
Bước 3: Cài đặt đồng hồ cho Router, ta dùng lệnh **Clock set** hh:mm:ss day mon year



Hình 2. 18: Gõ lệnh clock set + thời gian ngày tháng năm

Bước 4: Sử dụng lệnh **Show version**

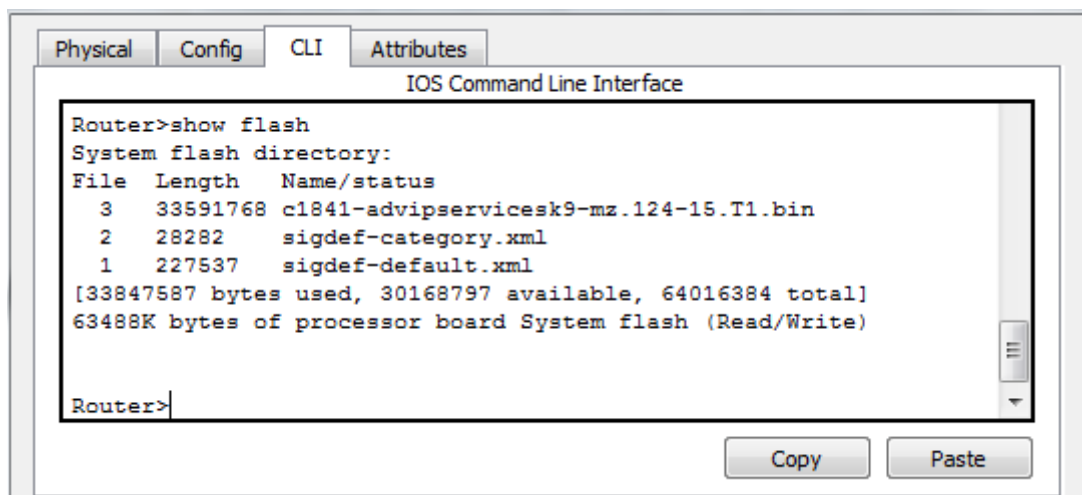
- Từ CLI, ta gõ lệnh show version



Hình 2. 19: Gõ lệnh Router>show version từ giao diện CLI

Bước 5: Sử dụng lệnh **Show flash**

- Từ CLI, ta gõ lệnh show flash



Hình 2. 20: Gõ lệnh Router>show flash từ giao diện CLI

3.5.Những sự cố thường gặp

Bảng 2. 5: những sự cố thường gặp của bài tập 2.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không tìm thấy router	Chọn sai tên router	Check vào Tab tên các router để xuất hiện tên router và chọn lại theo yêu cầu

Phần mềm Cisco Packet Tracer thiếu chức năng	Do phiên bản Cisco Packet Tracer đã cũ	Cập nhật phiên bản mới
Router đang chạy thì ngưng hoạt động	Đặt thời gian không đủ	Cài đặt thời gian phải đồng bộ với máy tính và đủ cho router vận hành
Ping không thông mạng	Do nhập sai tên lệnh	Kiểm tra đặt lại và nhập đúng tên lệnh cần tìm

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7. Đánh giá các bước thực hành

Bảng 2. 6: đánh giá các bước thực hành bài tập 2.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Khởi động router:	Chọn đúng router			
2	Bước 2: Cài đặt cấu hình cơ bản trên Router	Chọn đúng chế độ cấu hình			
3	Bước 3: Cài đặt đồng hồ cho Router, ta dùng lệnh Clock set hh:mm:ss day mon year	Đặt đúng thời gian cho đồng hồ			
4	Bước 4: Sử dụng lệnh Show version	Nhập đúng dòng lệnh			
5	Bước 5: Sử dụng lệnh Show flash	Nhập đúng dòng lệnh			

4.TÓM TẮT NỘI DUNG

- Các phương pháp thiết lập phiên kết nối CLI vào router.
- Sự khác nhau giữa 2 chế độ EXEC người dùng và EXEC đặc quyền
- Thiết lập phiên kết nối vào router bằng HyperTerminal.
- Truy cập vào router.
- Sử dụng chế độ trợ giúp của router trong giao diện dòng lệnh.
- Sử dụng cơ chế hỗ trợ soạn thảo câu lệnh.
- Gọi lại các câu lệnh đã sử dụng.
- Xử lý lỗi câu lệnh.
- Sử dụng lệnh show version.

5.CÂU HỎI VÀ BÀI TẬP

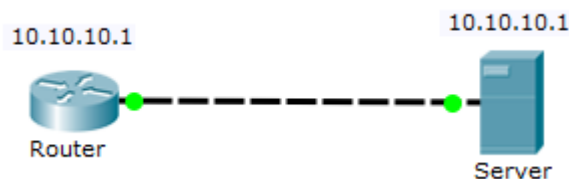
Câu hỏi:

Câu 1: Trình bày mục đích của IOS và giao diện người dùng của Router ?

Câu 2: Các đặc điểm và hoạt động của phần mềm IOS ?

Bài Tập:

Cho mô hình đơn giản gồm 1 PC kết nối với Router Cisco như hình :



- a. Chuyển từ chế độ EXEC người dùng sang chế độ EXEC đặc quyền trong Router.
- b. Nạp IOS cho Router Cisco từ Rommon.
- c. Backup and restore Router Cisco.

BÀI 3:CẤU HÌNH ROUTER

Mã bài MD 28-03

Thời gian: 10 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

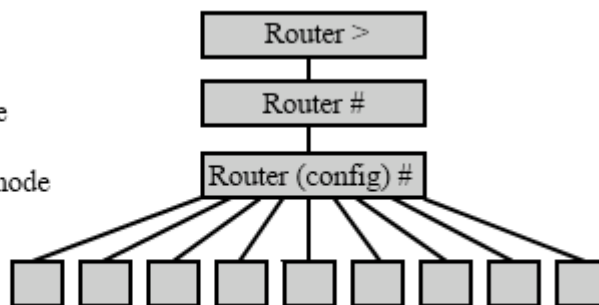
- Đặt tên cho router;
- Cài đặt mật mã cho router;
- Khảo sát các lệnh show;
- Cấu hình cổng Ethernet trên router;
- Thực hiện một số thay đổi trên router;
- Cấu hình câu chú thích cho các cổng giao tiếp trên router;
- Thực hiện các thao tác an toàn với máy tính;

II.NỘI DUNG CHÍNH

1. Cấu hình router.

1.1 Chế độ giao tiếp dòng lệnh CLI

- User EXEC mode
- Privileged EXEC mode
- Global configuration mode
- Specific configuration modes



Operating Environment	Prompt
Interface	Router(config-if)#
Subinterface	Router (config-subif)#
Controller	Router (config-controller)#
Map-list	Router (config-map-list)#
Map-class	Router (config-map-class)#
Line	Router (config-line)#
Router	Router (config-router)#
IPX-router	Router (config-ipx-router)#
Router-map	Router (config-router-map)#

Hình 3. 1: Giao diện dòng lệnh

- Tất cả các câu lệnh làm thay đổi cấu hình router đều xuất phát từ chế độ cấu hình toàn cục. Muốn thay đổi phần cấu hình đặc biệt nào của router thì chuyển vào chế độ chuyên biệt tương ứng. Các chế độ cấu hình chuyên biệt này đều là chế độ con của chế độ cấu hình toàn cục.
- Các câu lệnh được sử dụng trong chế độ cấu hình toàn cục là những câu

lệnh có tác động lên toàn bộ hệ thống. Sử dụng câu lệnh sau để di chuyển vào chế độ cấu hình toàn cục:

Chú ý: Sự thay đổi của dấu nhắc cho biết đang ở chế độ cấu hình toàn cục

Router # **configure terminal**

Router(config)#

- Chế độ cấu hình toàn cục là chế độ cấu hình chính. Từ chế độ này có thể chuyển vào các chế độ chuyên biệt như:

- Chế độ cấu hình cổng giao tiếp.
- Chế độ cấu hình đường truy cập.
- Chế độ cấu hình router.
- Chế độ cấu hình cổng con.
- Chế độ cấu hình bộ điều khiển.

- Khi chuyển vào chế độ cấu hình chuyên biệt nào thì dấu nhắc sẽ thay đổi tương ứng. Các câu lệnh trong đó chỉ có tác động đối với các cổng hay các tiến trình nào liên quan đến chế độ cấu hình đó thôi.

- Dùng lệnh exit để trở về chế độ cấu hình toàn cục hoặc dùng phím Ctrl-Z để quay về thẳng chế độ EXEC đặc quyền.

1.2 Đặt tên cho router

- Công việc đầu tiên khi cấu hình router là đặt tên cho router. Trong chế độ cấu hình toàn cục, với dòng lệnh sau:

Router(config)#**hostname Tokyo**

Tokyo (config)#

- Nhấn phím Enter để thực thi câu lệnh đổi từ tên mặc định (Router) sang tên vừa mới đặt (Tokyo).

1.3 Đặt mật mã cho router

- Mật mã được sử dụng để hạn chế việc truy cập vào router. Thông thường ta luôn đặt mật mã cho đường vty và console trên router. Ngoài ra mật mã còn được sử dụng để kiểm soát sự truy cập vào chế độ EXEC đặc quyền trên router. Khi đó, chỉ những người nào được phép mới có thể thực hiện việc thay đổi tập tin cấu hình trên router.

- Sau đây là các lệnh cần sử dụng để thực hiện việc đặt mật mã cho đường console:

Router(config)#**line console 0**

Router(config-line)#**password** <password>

Router(config-line)#**login**

- Chúng ta cũng cần đặt mật mã cho một hoặc nhiều đường vty để kiểm soát các user truy nhập từ xa vào router và Telnet. Thông thường Cisco router

có 5 đường vty với thứ tự từ 0 đến 4. Chúng ta thường sử dụng một mật mã cho tất cả các đường vty, nhưng đôi khi chúng ta nên đặt thêm mật mã riêng cho một đường để dự phòng khi cả 4 đường kia đều đang được sử dụng. Sau đây là các lệnh cần sử dụng để đặt mật mã cho đường vty:

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password <password>
```

```
Router(config-line)#login
```

- Mật mã **enable** và **enable secret** được sử dụng để hạn chế việc truy cập vào chế độ EXEC đặc quyền. Mật mã **enable** chỉ được sử dụng khi chúng ta cài đặt mật mã **enable secret** vì mật mã này được mã hoá còn mật mã **enable** thì không. Sau đây là các lệnh dùng để đặt mật mã **enable secret**:

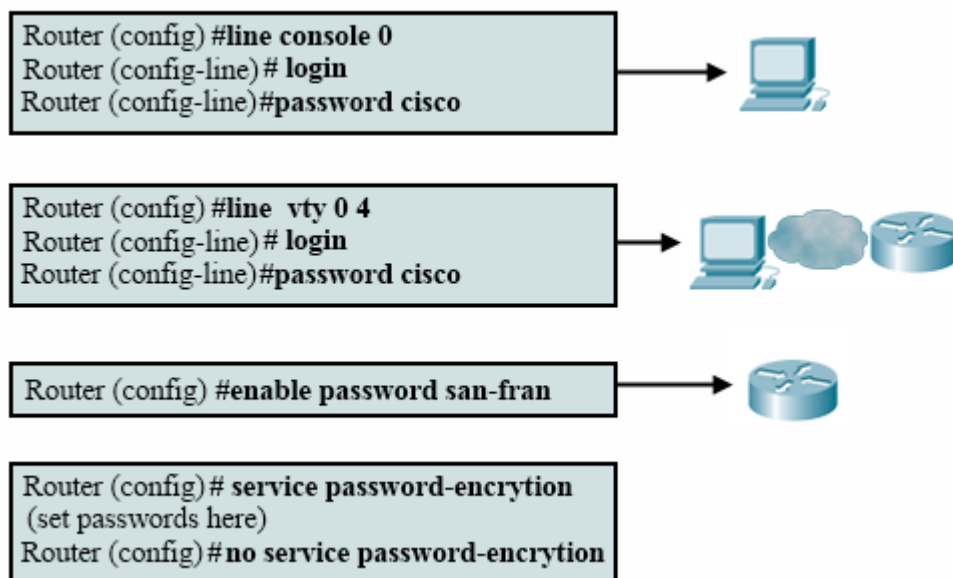
```
Router(config)#enable password <password>
```

```
Router(config)#enable secret <password>
```

- Đôi khi người quản trị sẽ thấy là rất không an toàn khi mật mã được hiển thị rõ ràng khi sử dụng lệnh **show running-config** hoặc **show startup-config**. Để tránh điều này người quản trị nên dùng lệnh sau để mã hoá tất cả các mật mã hiển thị trên tập tin cấu hình của router:

```
Router(config)#service password-encryption
```

- Lệnh **service password-encryption** sẽ áp dụng một cơ chế mã hoá đơn giản lên tất cả các mật mã chưa được mã hoá. Riêng mật mã **enable secret** thì sử dụng một thuật toán mã hoá rất mạnh là MD5.



Hình 3. 2: Lệnh đặt password

1.4 Kiểm tra bằng các lệnh show

- Có rất nhiều lệnh **show** được dùng để kiểm tra nội dung các tập tin trên router và để tìm ra sự cố. Trong cả hai chế độ EXEC đặc quyền và EXEC người dùng, khi gõ **show?** Để xem được danh sách các lệnh **show**. Dưới

nhiên là số lệnh **show** dùng được trong chế độ EXEC đặc quyền sẽ nhiều hơn trong chế độ EXEC người dùng.

- Show interface - hiển thị trạng thái của tất cả các cổng giao tiếp trên router. Để xem trạng thái của một cổng nào đó thì thêm tên và số thứ tự của cổng đó sau lệnh show interface. Ví dụ như: Router#**show interface serial 0/1**.
- Show controllers serial - hiển thị các thông tin chuyên biệt về phần cứng của các cổng serial.
- Show clock - hiển thị đồng hồ được cài đặt trên router.
- Show hosts - hiển thị danh sách tên và địa chỉ tương ứng.
- Show users - hiển thị tất cả các user đang kết nối vào router.
- Show history - hiển thị danh sách các câu lệnh vừa mới được sử dụng.
- Show flash – hiển thị thông tin bộ nhớ flash và tập tin IOS chứa trong đó.
- Show version - hiển thị thông tin về router và IOS đang chạy trên RAM.
- Show ARP - hiển thị bảng ARP trên router.
- Show protocol - hiển thị trạng thái toàn cục và trạng thái của các cổng giao tiếp đã được cấu hình giao thức lớp 3.
- Show startup-configuration - hiển thị tập tin cấu hình đang chạy trên RAM.

1.5 Cấu hình cổng serial

- Cấu hình cổng serial bằng đường console hoặc vty. Sau đây là các bước cần thực hiện khi cấu hình cổng serial:

- **Bước 1:** Vào chế độ cấu hình toàn cục.
- **Bước 2:** Vào chế độ cấu hình cổng serial.
- **Bước 3:** Khai báo địa chỉ và subnet mask.
- **Bước 4:** Đặt tốc độ clock nếu đầu cáp cắm vào cổng serial là DCE. Nếu đầu cáp là DTE thì chúng ta có thể bỏ qua này.
- **Bước 5:** Khởi động serial.

- Mỗi một cổng serial đều phải có một địa chỉ IP và subnet mask để chúng có thể định tuyến các gói IP. Để cấu hình địa chỉ IP chúng ta dùng lệnh sau:

```
Router(config)#interface serial 0/0  
Router(config)#ip address <ip address> <netmask>
```

- Cổng serial cần phải có tín hiệu clock để điều khiển thời gian thực hiện thông tin liên lạc. Trong hầu hết các trường hợp, thiết bị DCE, ví dụ như CSU, sẽ là thiết bị cung cấp tín hiệu clock. Mặc định thì Cisco router là thiết bị DTE nhưng chúng ta có thể cấu hình chúng thành thiết bị DCE.

- Trong môi trường làm lab thì các đường liên kết serial được kết nối trực tiếp với nhau. Do đó phải có một đầu là DCE để cấp tín hiệu clock. dùng lệnh **clockrate** để cài đặt tốc độ clock. Sau đây là các tốc độ clock mà có thể đặt cho router (đơn vị của tốc độ clock là bit/s): 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000. Tuy nhiên sẽ có một số tốc độ không sử dụng được tùy theo khả năng vật lý của từng cổng serial.

- Mặc định thì các cổng giao tiếp trên router đều đóng. Muốn mở hay khởi động các cổng này thì phải dùng lệnh **no shutdown**. Muốn đóng cổng lại để bảo trì hoặc xử lý sự cố thì dùng lệnh **shutdown**.

- Trong môi trường làm lab, tốc độ clock thường được sử dụng là 56000. Sau đây là các lệnh được sử dụng để cài đặt tốc độ clock và khởi động cổng serial:

```
Router(config)#interface serial 0/0  
Router(config-if)#clock rate 56000  
Router(config-if)#no shutdown
```

1.6 Thêm bớt, dịch chuyển và thay đổi tập tin cấu hình

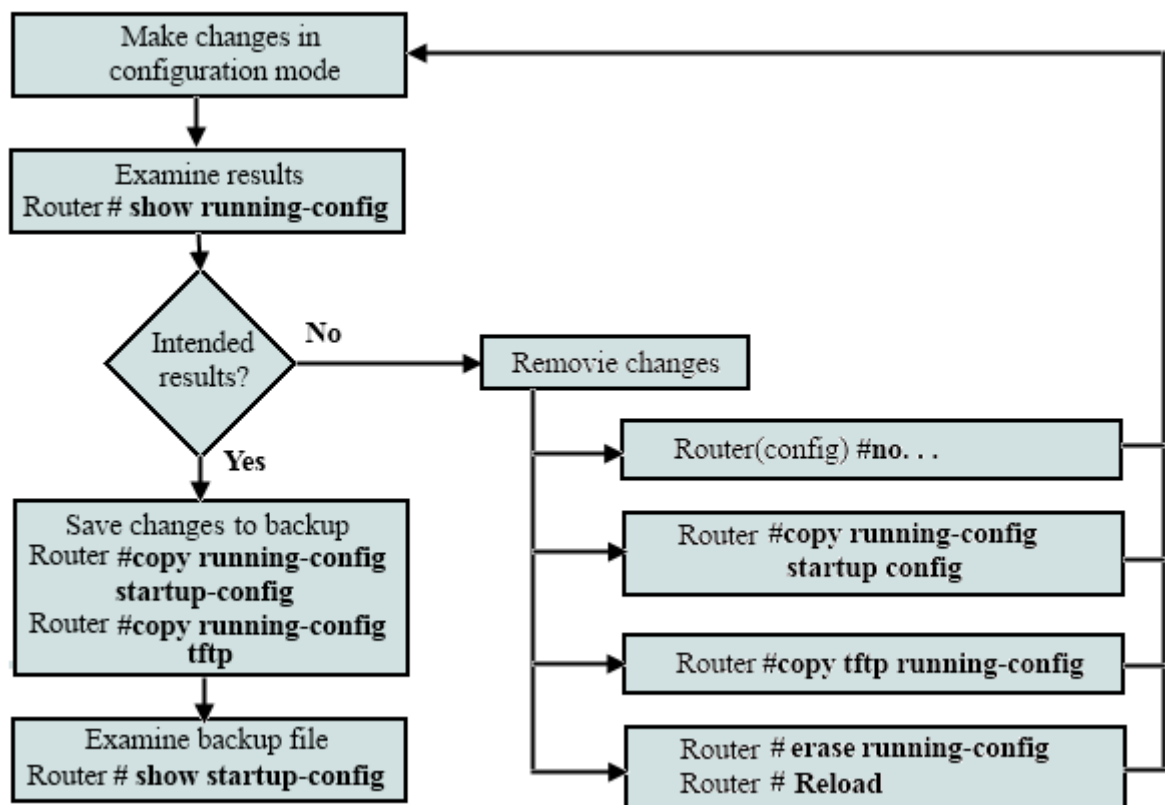
- Chỉnh sửa tập tin cấu hình thì phải di chuyển vào đúng chế độ cấu hình và thực hiện cần thiết. Ví dụ: nếu cần mở một cổng nào đó trên router thì trước hết phải vào chế độ cấu hình toàn cục, sau đó vào chế độ cấu của cổng đó rồi dùng lệnh **no shutdown**.

- Để kiểm tra những gì vừa mới thay đổi, dùng lệnh **show running-config**. Lệnh này sẽ hiển thị nội dung của tập tin cấu hình hiện tại. Nếu kết quả hiển thị có những chi tiết không đúng thì có thể chỉnh sửa lại bằng cách thực hiện một hoặc nhiều cách sau:

- Dùng dạng **no** của các lệnh cấu hình.
- Khởi động lại router với tập tin cấu hình nguyên thủy trong NVRAM.
- Chép tập tin cấu hình dự phòng từ TFTP server.
- Xóa tập tin cấu hình khởi động bằng lệnh **erase startup-config**, sau đó khởi động lại router và vào chế độ cài đặt.

- Để lưu tập tin, cấu hình hiện tại thành tập tin cấu hình khởi động lưu trong NVRAM, dùng lệnh như sau:

```
Router#copy running-config startup-config
```



Hình 3. 3: Lệnh show running- config

1.7 Cấu hình cổng Ethernet

- Tương tự như cổng serial, chúng ta có thể cấu hình cổng Ethernet bằng đường console hoặc vty.
- Mỗi cổng Ethernet cũng cần phải có một địa chỉ IP và subnet mask để có thể thực hiện định tuyến các gói IP qua cổng đó.
- Sau đây là các bước thực hiện cấu hình Ethernet:
 - Vào chế độ cấu hình toàn cục.
 - Vào chế độ cấu hình cổng Ethernet.
 - Khai báo địa chỉ và subnet mask.
 - Khởi động cổng Ethernet.
- Mặc định là các cổng trên router đều đóng. Do đó, phải dùng lệnh **no shutdown** để mở hay khởi động cổng. Cần đóng cổng lại để bảo trì hay xử lý sự cố thì dùng lệnh **shutdown**.

```

Router(config)#interface e0
Router(config-if)#ip address 183.8.126.2 255.255.255.128
Router(config-if)#no shutdown
  
```

Hình 3. 4: Lệnh shutdown

2. Hoàn chỉnh cấu hình router.

2.1 Tầm quan trọng của việc chuẩn hoá tập tin cấu hình

- Trong một tổ chức việc phát các quy định dành cho các tập tin cấu hình

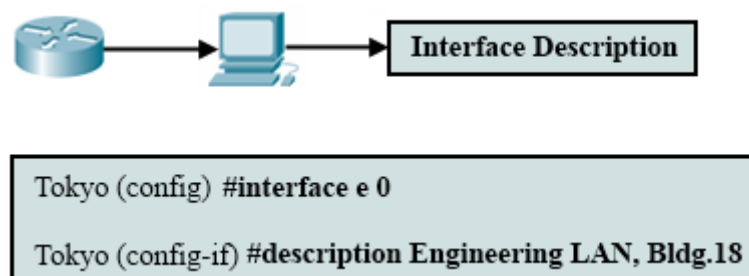
là rất cần thiết. Từ đó ta có thể kiểm soát được các tập tin nào cần bảo trì, lưu các tập tin ở đâu và như thế nào.

- Các quy định này có thể là những quy định được ứng dụng rộng rãi hoặc cũng có thể chỉ có giá trị trong một phạm vi nào đó. Nếu không có một quy định chung cho tổ chức của mình thì hệ thống mạng của sẽ trở nên lộn xộn và không đảm bảo được hoạt động thông suốt.

2.2 Câu chú thích cho các cổng giao tiếp

- Trên các cổng giao tiếp nên ghi chú lại một số thông tin quan trọng, ví dụ như chỉ số mạch mà cổng này kết nối vào, hay thông tin vào router khác, về phân đoạn mạng mà cổng này kết nối đến. Dựa vào các câu chú thích này, người quản trị mạng có thể biết được là cổng giao tiếp này kết nối vào đâu.

- Câu chú thích chỉ đơn giản là ghi chú thêm cho các cổng giao tiếp, ngoài ra nó hoàn toàn không có tác động gì đối với hoạt động của router. nên viết câu chú thích theo một định dạng chung và mỗi cổng giao tiếp có một câu chú thích riêng. Tùy theo cấu trúc mạng và quy ước chung, người quản trị có thể quyết định là ghi chú những thông tin nào liên quan đến cổng giao tiếp để giúp cho tập tin cấu hình được rõ ràng hơn, giúp cho việc xác định sự cố được nhanh hơn.



Hình 3. 5: Câu chú thích cho các cổng giao tiếp

2.3 Cấu hình câu chú thích cho cổng giao tiếp

- Trước tiên phải vào chế độ cấu hình toàn cục. Rồi từ chế độ cấu hình toàn cục chuyển vào chế độ cấu hình cổng giao tiếp. Tại đây gõ lệnh **description** và câu chú thích mà muốn.

- Sau đây là các bước để cấu hình câu chú thích cho cổng giao tiếp:

- **Bước 1:** Vào chế độ cấu hình toàn cục bằng lệnh **configure terminal**.
- **Bước 2:** Vào chế độ cấu hình cổng giao tiếp (ví dụ là cổng Ethernet0): **interface** giao tiếp (ví dụ là cổng Ethernet 0): **interface Ethernet 0**.
- **Bước 3:** Nhập lệnh **description** và theo sau là câu chú thích.
- **Bước 4:** Thoát khỏi chế độ cấu hình giao tiếp để trở về chế độ EXEC đặc quyền bằng cách nhấn phím **Ctrl-Z**.
- **Bước 5:** Lưu lại cấu hình vừa rồi vào NVRAM bằng lệnh **copy running-config startup- config**.

- Sau đây là 2 ví dụ về cách viết câu chú thích:

Interface Ethernet 0

Description LAN Engineering, Bldg.2

Interface serial 0

Description ABC network 1, circuit 1

```
LAB_A# config terminal
Enter configuration commands, one per line. End with
CNTL_Z
LAB_A (config)# interface Ethernet 0
LAB_A (config-if)#description LAN Engineerinnng, Bldg. 2
```

2.4 Thông điệp đăng nhập.Cấu hình thông điệp đăng nhập (MOTD)

- Thông điệp đăng nhập được hiển thị khi đăng nhập vào hệ thống. Loại thông điệp này rất hữu dụng khi cần cảnh báo trước khi đến giờ tắt hệ thống mạng.

- Tất cả mọi người đều có thể nhìn thấy thông điệp đăng nhập. Cho nên dùng các thông điệp mạng tính cảnh báo, thu hút sự chú ý. Còn những thông điệp để “chào đón” mọi người đăng nhập vào router là không thích hợp lắm.

- Ví dụ một thông điệp như sau: “This is a secure system, authorized access only!” (Đây là hệ thống được bảo mật, chỉ dành cho những người có thẩm quyền!) được sử dụng để cảnh báo những vị khách viếng thăm bất hợp pháp.

```
LAB_A con0 is now available
Press RETURN to get started.
This is a secure system. Authorizes Access ONLY!!!
User Access Verification
Password:
LAB_A>enable
Password:
LAB_A#
```

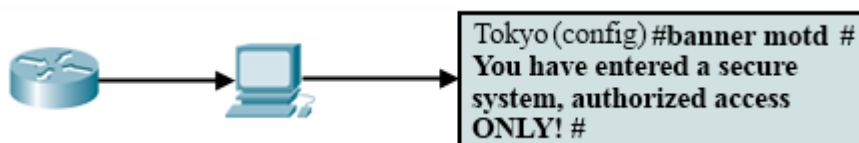
Hình 3. 6: Thông điệp đăng nhập

- Để cấu hình thông điệp MOTD, vào chế độ cấu hình toàn cục. Tại đây dùng lệnh **banner motd**, cách một khoảng trắng, nhập ký tự phân cách ví dụ như ký tự #, rồi viết câu thông báo, kết thúc bằng cách nhập ký tự phân cách một lần nữa.

- Sau đây là các bước thực hiện để cấu hình thông điệp MOTD:

➤ **Bước 1:** Vào chế độ cấu hình toàn cục bằng lệnh **configure terminal**.

- **Bước 2:** Nhập lệnh như sau: `banner motd #The message of the day goes here #`.
- **Bước 3:** Lưu cấu hình vừa rồi bằng lệnh **`copy running-config startup-config`**.



Hình 3. 7: Cấu hình đăng nhập

2.5 Phân giải tên máy

- Phân giải tên máy là quá trình máy tính phân giải từ tên máy thành địa chỉ IP tương ứng.
- Để có thể liên hệ với các thiết bị IP khác bằng tên thì các thiết bị mạng như router cũng cần phải có khả năng phân giải tên máy thành địa chỉ IP. Danh sách giữa tên máy và địa chỉ IP tương ứng được gọi là bảng host.
- Bảng host có thể bao gồm tất cả các thiết bị mạng trong tổ chức của mình. Mỗi một địa chỉ IP có một tên máy tương ứng. Phần mềm Cisco IOS có một vùng đệm để lưu tên máy và địa chỉ tương ứng. Vùng bộ đệm này giúp cho quá trình phân giải tên thành địa chỉ được nhanh hơn.
- Tuy nhiên tên máy ở đây không giống như tên DNS, nó chỉ có ý nghĩa đối với router mà nó được cấu hình mà thôi. Người quản trị mạng có thể cấu hình bảng host trên router với bất kỳ tên nào với IP nào và các thông tin này chỉ có ý nghĩa đối với router đó mà thôi.
- Sau đây là ví dụ về câu lệnh phân giải tên máy trên router:

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

2.6 Cấu hình bảng host

- Để khai báo tên cho các địa chỉ IP, đầu tiên vào chế độ cấu hình toàn cục. Tại đây dùng lệnh **`ip host`**, theo sau là tên của thiết bị và tất cả các IP của nó. Như vậy tên máy này sẽ ánh xạ với từng địa chỉ IP của các cổng trên thiết bị đó. Khi đó có thể dùng lệnh ping hay telnet tới thiết bị đó bằng tên của thiết bị hay địa chỉ IP tương ứng đều được.
- Sau đây là các bước thực hiện cấu bảng host:
- **Bước 1:** Vào chế độ cấu hình toàn cục của router.
- **Bước 2:** Nhập lệnh **`ip host`** theo sau là tên của router và tất cả các địa chỉ IP của các cổng trên router đó.
- **Bước 3:** Tiếp tục nhập tên và địa chỉ IP tương ứng của các router khác trong mạng.

2.7 Lập hồ sơ và lưu dự phòng tập tin cấu hình

- Tập tin cấu hình của các thiết bị mạng sẽ quyết định sự hoạt động của hệ thống. Công việc quản lý tập tin cấu hình của các thiết bị bao gồm các công việc sau:

- Lập danh sách và so sánh với tập tin cấu hình trên các thiết bị đang hoạt động.
- Lưu dự phòng các tập tin cấu hình lên server mạng.
- Thực hiện cài đặt và nâng cấp các phần mềm.

- Chúng ta cần lưu dự phòng các tập tin cấu hình để sử dụng trong trường hợp có sự cố. Tập tin cấu hình có thể được lưu trên server mạng, ví dụ như TFTP server, hoặc là lưu trên đĩa và cất ở nơi an toàn. Ngoài ra chúng ta cũng nên lập hồ sơ đi kèm với các tập tin này.

2.8 Cắt, dán và chỉnh sửa tập tin cấu hình

- Chúng ta có thể dùng lệnh **copy running-config tftp** để sao chép tập tin cấu hình đang chạy trên router vào TFTP server. Sau đây là các bước thực hiện:

- **Bước 1:** nhập lệnh **copy running-config tftp**.
- **Bước 2:** nhập địa chỉ IP của máy mà chúng ta sẽ lưu tập tin cấu hình lên đó.
- **Bước 3:** nhập tên tập tin.
- **Bước 4:** xác nhận lại câu lệnh bằng cách trả lời “yes”.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write [tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!! [OK]
```

- Chúng ta có thể sử dụng tập tin cấu hình lưu trên server mạng để cấu hình cho router.

- Để thực hiện điều này làm theo các bước sau:

- **Bước 1:** Nhập lệnh **copy tftp running-config**.
- **Bước 2:** Ở dấu nhắc tiếp theo chọn loại tập tin cấu hình máy hay tập tin cấu hình mạng. Tập tin cấu hình mạng có chứa các lệnh có thể thực thi cho tất cả các router và server trong mạng. Còn loại tập tin cấu hình máy thì chỉ s các lệnh thực thi cho một router mà thôi. Ở dấu nhắc kế tiếp, nhập địa chỉ IP của máy nào mà đang lưu tập tin cấu hình trên đó. Ví dụ: router được cấu hình từ TFTP server có địa chỉ IP là 131.108.2.155.
- **Bước 3:** Sau đó nhập tên của tập tin hoặc là chấp nhận lấy tên mặc định.

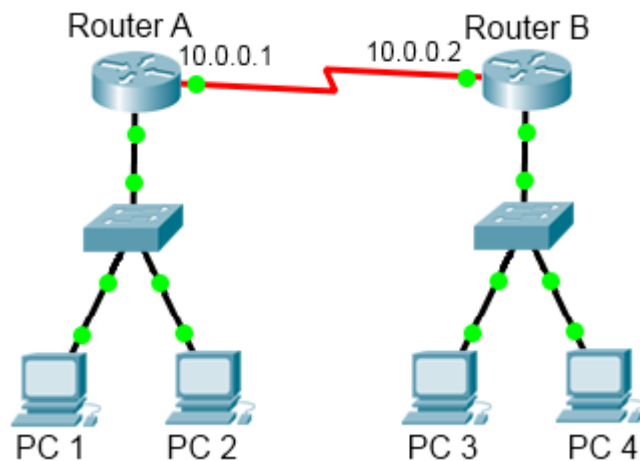
Tên của tập tin theo quy tắc của UNIX. Tên mặc định cho loại tập tin cấu hình máy là hostname-config, còn tên mặc định cho loại tập tin cấu hình mạng là network-config. Trong môi trường DOS thì tên tập tin bị giới hạn với 8 ký tự và 3 ký tự mở rộng (ví dụ như: router.cfg). Cuối cùng xác nhận lại tất cả các thông tin vừa rồi. Lưu ý trên hình thì sẽ thấy là dấu nhắc chuyển ngay sang tên Tokyo. Điều này chứng tỏ là router được cấu hình lại ngay sau khi tập tin cấu hình vừa được tải xuống.

- Tập tin cấu hình trên router cũng có thể được lưu vào đĩa bằng cách sao chép dưới dạng văn bản rồi lưu vào đĩa mềm hoặc đĩa cứng. Khi nào cần chép trở lại router thì dùng chức năng soạn thảo cơ bản của chương trình mô phỏng thiết bị đầu cuối để cắt dán các dòng lệnh vào router.

3.BÀI TẬP THỰC HÀNH 3.1

3.1.Mô hình

- Cho mô hình mạng như hình 3.11:



Hình 3. 8: Mô hình PC kết nối Router

3.2.Yêu cầu

- + Đặt tên và mật mã cho Router A và Router B.
- + Cấu hình cổng Serial và đặt địa chỉ IP và Subnet Mask.
- + Cấu hình câu chú thích cho cổng Serial bằng lệnh **description**.
- + Sử dụng lệnh **copy running- config tftp** để sao chép tập tin cấu hình đang chạy trên router vào TFTP server .

3.3.Chuẩn bị:

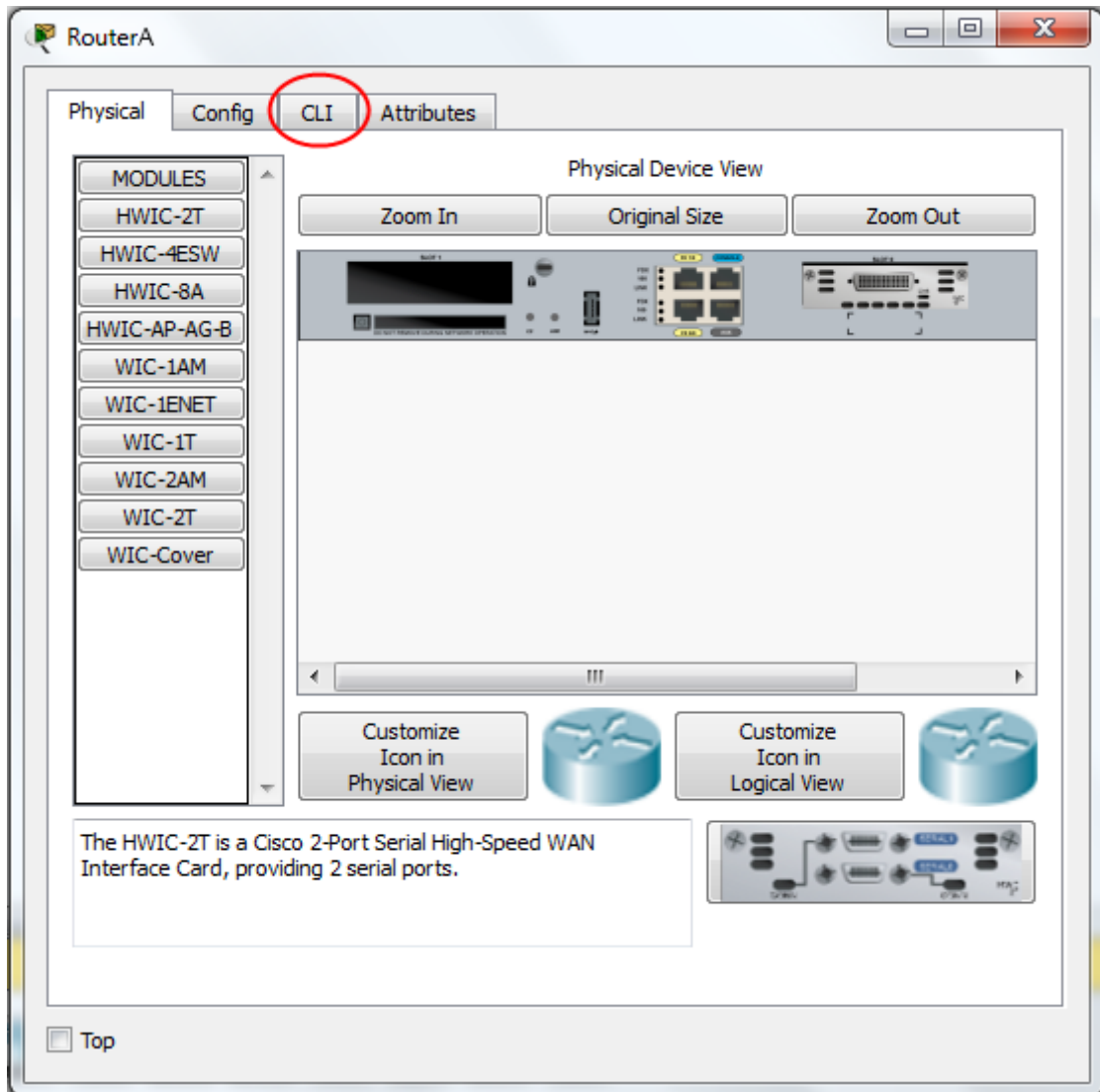
Bảng 3. 1: chuẩn bị phần mềm cài đặt, máy tính, router thực hành bài tập 3.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	4	
3	Router ảo	Cái	2	
4	Switch	Cái	2	

3.4. Các bước thực hành:

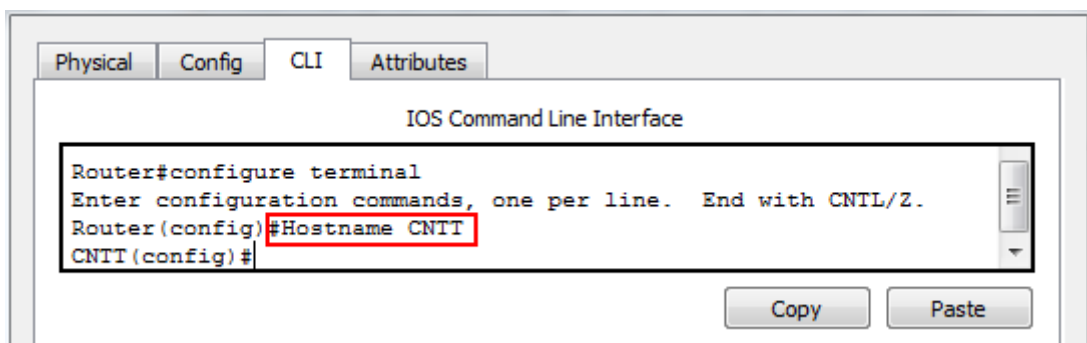
Bước 1: Đặt tên cho Router A

- Nhấn vào Router A, sau đó chuyển sang tab CLI.



Hình 3. 9: Giao diện khi nhấn vào Router A

- Gõ lệnh **#configure terminal** để vào chế độ cấu hình toàn cục, sau đó gõ lệnh **Hostname [Tên Router]** để đặt tên cho Router.

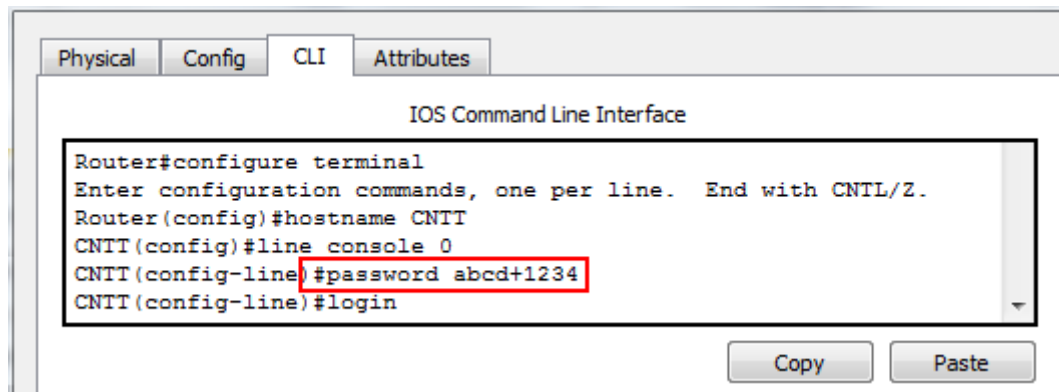


Hình 3. 10: Giao diện khi nhấn vào Router A

- Làm tương tự với Router B.

Bước 2: Cài đặt mật mã cho Router A:

- Từ giao diện CLI, ta gõ lệnh **Line console 0** sau đó Enter.
- Nhập tiếp lệnh **password [Mật mã]**, sau đó gõ lệnh đăng xuất **login**.

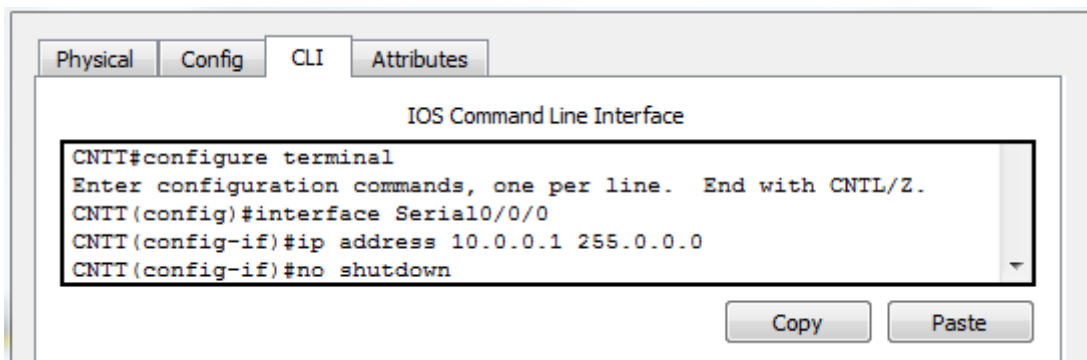


Hình 3. 11: Đặt mật mã cho Router A

- Làm tương tự với Router B.

Bước 3: Cấu hình cổng Serial cho Router A

- Từ chế độ cấu hình toàn cục, ta vào chế độ cấu hình cổng serial bằng cách gõ lệnh **interface [cổng Serial]**
- Sau đó khai báo địa chỉ và subnet mask bằng lệnh **ip address <địa chỉ ip> <subnet mask>**

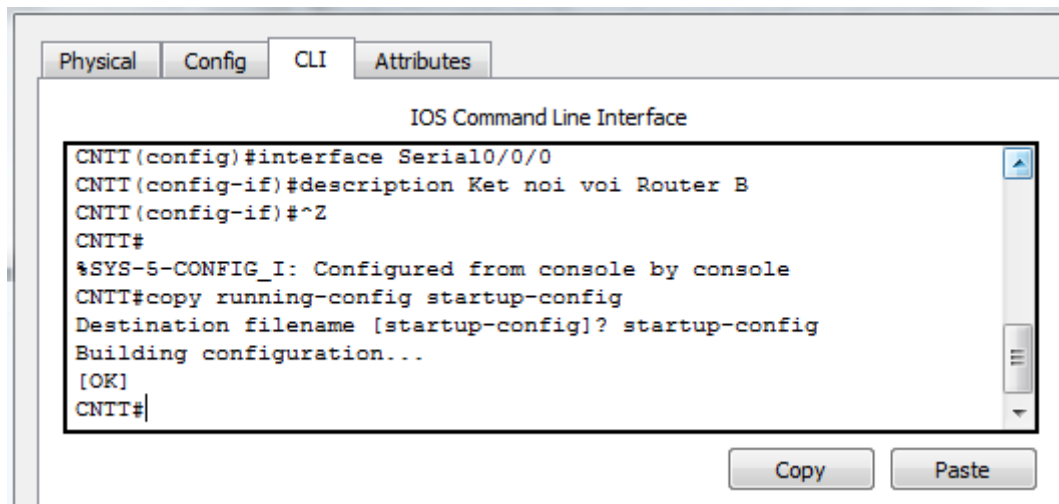


Hình 3. 12: Cấu hình cổng Serial

- Cuối cùng khởi động cổng Serial bằng lệnh **no shutdown**.

Bước 4: Cấu hình câu chú thích cho cổng Serial:

- Đầu tiên ta vào chế độ cấu hình toàn cục bằng lệnh **configure terminal**.
- Sau đó ta vào chế độ cấu hình cổng Serial **interface Serial 0**.
- Nhập lệnh **description [Nội dung câu chú thích]**

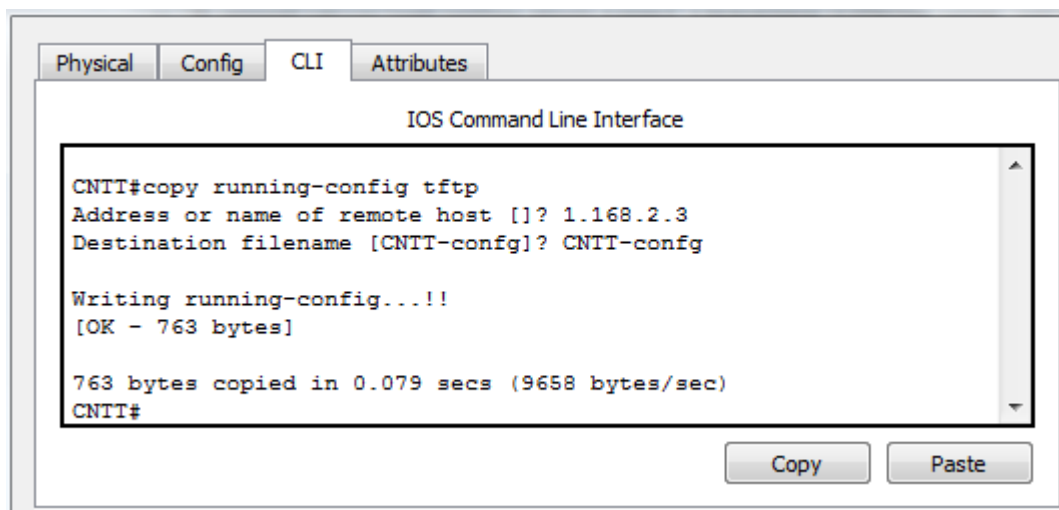


Hình 3. 13: Cấu hình câu chú thích cho cổng Serial

- Thoát khỏi chế độ cấu hình giao tiếp để trở về chế độ EXEC đặc quyền bằng cách nhấn phím **Ctrl-Z**.
- Lưu lại cấu hình vừa rồi vào NVRAM bằng lệnh **copy running-config startup-config**.

Bước 5: Sao chép tập tin cấu hình đang chạy trên router A vào TFTP server.

- Đầu tiên nhập lệnh **copy running-config tftp**.
- Nhập địa chỉ IP của máy PC1 là 1.168.2.3
- Xác nhận lệnh lần nữa tại dòng Destination filename [CNTT-config]? ta nhập theo nội dung trong [] là: CNTT-config



Hình 3. 14: Sao chép tập tin trên Router A

3.5.Những sự cố thường gặp

Bảng 3. 2: những sự cố thường gặp của bài tập 3.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không chấp nhận	Password thiếu ký tự và	Đặt đúng số ký tự

password	không đủ độ phức tạp	quy định và có độ phức tạp. Ví dụ: 123+abc@
Không nhìn thấy cổng Serial	Chưa cập nhật phần mềm	Cập nhật lại
Không cho sao chép	Chọn chưa đúng cấu hình	Chọn lại cấu hình và nhập đúng lệnh

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7. Đánh giá các bước thực hành

Bảng 3. 3: đánh giá các bước thực hành bài tập 3.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Đặt tên cho Router A	Đặt đúng tên			
2	Bước 2: Cài đặt mật mã cho Router A	Nhập đúng lệnh password			
3	Bước 3: Cấu hình cổng Serial cho Router A	Chọn đúng cổng			
4	Bước 4: Cấu hình câu chú thích cho	Nhập đúng dòng lệnh			

	cổng Serial				
5	Bước 5: Sao chép tập tin cấu hình đang chạy trên router A vào TFTP server.	Nhập đúng dòng lệnh và đúng địa chỉ IP			

4.TÓM TẮT NỘI DUNG

- Xây dựng một cấu hình chuẩn là yếu tố quan trọng để thành công trong việc bảo trì bất kỳ hệ thống mạng của một tổ chức nào.
- Câu chú thích cho các cổng giao tiếp có thể mang một số thông tin quan trọng giúp cho người quản trị mạng nắm được cấu trúc hệ thống mạng và xử lý sự cố nhanh hơn.
- Thông điệp đăng nhập sẽ cung cấp các thông báo cho người dùng khi họ đăng nhập vào router.
- Phân giải tên máy thành địa chỉ IP cho phép router có thể chuyển đổi nhanh từ máy ra địa chỉ.
- Công việc lập hồ sơ và lưu dự phòng tập tin cấu hình là hết sức quan trọng để bảo đảm cho hệ thống mạng luôn hoạt động thông suốt.

5.CÂU HỎI VÀ BÀI TẬP

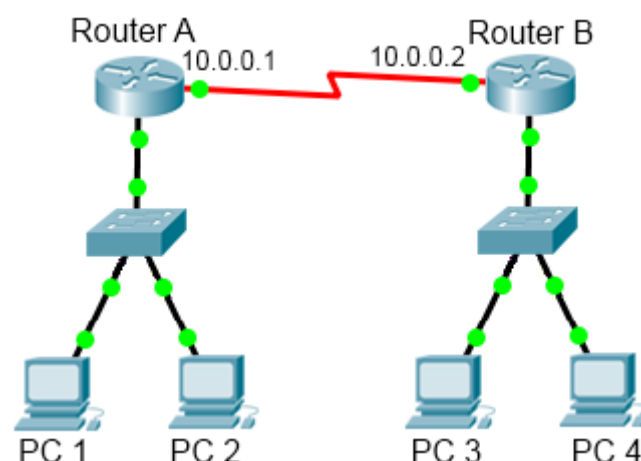
Câu hỏi:

Câu 1: Trình bày tầm quan trọng của việc chuẩn hoá tập tin cấu hình?

Câu 2: Phân giải tên máy là gì? Cho ví dụ về phân giải tên máy?

Bài tập:

Cho mô hình mạng như hình :



- Reset lại password cho Router A và Router B.
- Cấu hình cổng Ethernet cho 2 Router.
- Cấu hình SSH trên 2 Router Cisco.

BÀI 4:CẬP NHẬT THÔNG TIN TỪ CÁC THIẾT BỊ KHÁC

Mã bài MD 28-04

Thời gian: 5 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Bật và tắt CDP;
- Sử dụng lệnh Show cdp neighbors;
- Xác định các thiết bị lân cận kết nối vào các cổng;
- Ghi nhận thông tin và địa chỉ mạng của các thiết bị lân cận;
- Thiết lập và kiểm tra kết nối Telnet;
- Thực hiện các thao tác an toàn với máy tính;

II.NỘI DUNG CHÍNH

1. Kết nối và khám phá các thiết bị lân cận.

1.1 Giới thiệu về CDP

- CDP là giao thức lớp 2 kết nối với lớp vật lý ở dưới và lớp mạng ở trên như hình vẽ. CDP được sử dụng để thu thập thông tin từ các thiết bị lân cận, ví dụ như thiết bị đó là loại thiết bị nào, trên thiết bị đó cổng nào là cổng kết nối và kết nối vào cổng nào trên thiết bị của chúng ta, phiên bản phân cứng của thiết bị đó là gì...CDP là giao thức hoạt động độc lập với môi trường truyền mạng và có thể chạy trên tất cả các thiết bị của Cisco trên nền giao thức truy cập mạng con SNAP (Subnet Access Protocol).

- Khi thiết bị Cisco được bật lên, CDP tự động hoạt động và cho phép thiết bị dò tìm các thiết bị lân cận khác cùng chạy CDP. CDP hoạt động ở lớp liên kết dữ liệu và cho phép 2 thiết bị thu thập thông tin lẫn nhau cho dù 2 thiết bị này có thể chạy giao thức lớp mạng khác nhau.

- Mỗi thiết bị được cấu hình CDP sẽ gửi một thông điệp quảng cáo theo định kỳ cho các router khác. Mỗi thông điệp như vậy phải có ít nhất một địa chỉ mà thiết bị đó có thể nhận được thông điệp của giao thức quản lý mạng cơ bản SNMP (Simple Network Management Protocol) thông qua địa chỉ đó. Ngoài ra, mỗi thông điệp quảng cáo còn có “thời hạn sống” hoặc là thời hạn lưu giữ thông tin. Đây là khoảng thời gian cho các thiết bị lưu giữ thông tin nhận được trước khi xóa bỏ thông tin đó đi. Bên cạnh việc phát tin thông điệp, mỗi thiết bị cũng lắng nghe theo định kỳ để nhận thông điệp từ các thiết bị lân cận khác để thu thập thông tin về chúng.

1.2 Thông tin thu nhận được từ CDP

- CDP được sử dụng chủ yếu để phát hiện tất cả các thiết bị Cisco khác kết nối trực tiếp vào thiết bị của chúng ta. sử dụng lệnh **show cdp neighbors** để hiển thị thông tin về các mạng kết nối trực tiếp vào router. CDP cung cấp thông tin về từng thiết bị CDP lắng nghe bằng cách truyền thông báo CDP

mang theo các giá trị “type length” (TLVs).

- TLVs được hiển thị bởi lệnh **show cdp neighbors** sẽ bao gồm các thông tin về:

- Device ID: Chỉ số danh định (ID) của thiết bị láng giềng.
- Local giềng, interface: Cổng trên thiết bị của chúng ta kết nối đến thiết bị láng giềng.
 - Hold time: thời hạn lưu giữ thông tin cập nhật.
 - Capability: loại thiết bị.
 - Platform: phiên bản phần cứng của thiết bị.
 - Port ID: chỉ số danh định (ID) của cổng trên thiết bị láng giềng kết nối vào thiết bị của chúng ta.
 - VTP management domain name: tên miền quản lý của VTP (chỉ có ở CDPv2).
 - Native VLAN: VLAN mặc định trên router (chỉ có ở CDPv2).
- Half/Full duplex: chế độ hoạt động song công hay bán song công.

1.3 Chạy CDP, kiểm tra và ghi nhận các thông tin CDP

Bảng 4. 1: thông tin CDP

Lệnh	Chế độ cấu hình của router để thực hiện câu lệnh	Chức năng của câu lệnh
Cdp run	Chế độ cấu hình toàn cục	Khởi động cdp trên router.
Cdp enable	Chế độ cấu hình cổng giao tiếp.	Khởi động CDP trên cổng giao tiếp tương ứng
Clear cdp counters	Chế độ EXEC người dùng	Xoá đồng hồ đếm lưu lượng trở về 0
Show cdp entry (&/device-name [*][protocol/version])	Chế độ EXEC đặc quyền	Hiển thị thông tin về một thiết bị láng giềng mà ta cần. Thông tin hiển thị có thể được giới hạn theo giao thức hay theo phiên bản.
Show cdp	Chế độ EXEC đặc quyền	Hiển thị khoảng thời gian giữa các lần phát thông điệp quảng cáo CDP, số phiên bản và thời gian còn hiệu lực của các thông điệp này trên từng cổng của router.

Show cdp interface [type number]	Chế độ EXEC đặc quyền	Hiển thị thông tin về những cổng có chạy CDP.
Show cdp neighbors [type number] [detail]	Chế độ EXEC đặc quyền	Hiển thị các thông tin về những thiết bị mà CDP phát hiện được: loại thiết bị, tên thiết bị, thiết bị đó kết nối vào cổng nào trên thiết bị của chúng ta. Nếu có sử dụng từ khoá detail thì bạn sẽ có thêm thông tin về VLAN ID, chế độ hoạt động song công, tên miền VTP.

1.4 Xây dựng bản đồ mạng

- CDP là một giao thức được thiết kế và hoạt động khá nhẹ, đơn giản. Các gói CDP có kích thước nhỏ nhưng lại mang nhiều thông tin hữu ích về các thiết bị láng giềng Cisco.
- có thể sử dụng các thông tin này để xây dựng sơ đồ mạng của các thiết bị. có thể Telnet vào các thiết bị láng giềng rồi dùng lệnh **show cdp neighbors** để tìm tiếp các thiết bị khác kết nối vào thiết bị này.

1.5 Tắt CDP

- Để tắt toàn bộ CDP trên router, dùng lệnh **no cdp run** chế độ cấu hình toàn cục. Khi đã tắt toàn bộ CDP thì không có cổng nào trên router còn chạy được.
- Đối với Cisco IOS phiên bản 10.3 trở đi, CDP chạy mặc định trên tất cả các cổng có thể gửi và nhận thông tin CDP. Tuy nhiên cũng có một số cổng như cổng Asynchronous chẳng hạn thì mặc định là CDP tắt trên các cổng này. Nếu CDP đang bị tắt trên một cổng nào đó thì có thể khởi động lại CDP bằng lệnh **cdp enable** trong chế độ cấu hình cổng giao tiếp tương ứng. Còn nếu muốn tắt CDP trên một cổng nào đó thì dùng lệnh **no cdp enable** trong chế độ cấu hình cổng đó.

```

Rtl#show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Rtl#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rtl(config)#no cdp run
Rtl(config)#^Z
Rtl#show cdp
%CDP is not enable
Rtl#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z
Rtl(config)#cdp run

```

Hình 4. 1: Lệnh no cdp enable

1.6 Xử lý sự cố của CDP

Bảng 4. 2: mô tả lệnh CDP

Lệnh	Mô tả
Clear cdp table	Xoá bảng thông tin của CDP về các thiết bị láng
Clear cdp counters	Xoá bộ đếm lưu lượng trở về 0.
Show cdp traffic	Hiển thị bộ đếm của CDP, bao gồm số lượng gói CDP gửi và nhận, số lượng lỗi checksum
Show debugging	Hiển thị thông tin về các loại debug đang chạy trên
Debug cdp adjacency	Kiểm tra thông tin CDP về các thiết bị láng giềng
Debug cdp events	Kiểm tra các hoạt động của CDP
Debug cdp ip	Kiểm tra thông tin CDP IP
Debug cdp packets	Kiểm tra thông tin về các gói CDP
Cdp timer	Cài đặt thời gian định kỳ gửi gói CDP cập nhật
Cdp holdtime	Cài đặt thời gian lưu giữ thông tin cho các gói CDP cập nhật được phát đi
Show cdp	Hiển thị thông tin toàn cục của CDP, bao gồm thời gian cập nhật và thời gian lưu giữ thông tin

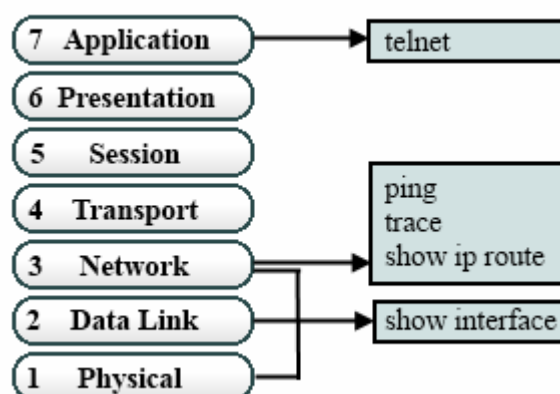
2. Thu thập thông tin về các thiết bị ở xa.

2.1 Telnet

- Telnet là giao thức giả lập đầu cuối ảo nằm trong bộ giao thức TCP/IP. Nó cho phép thiết lập kết nối từ xa vào thiết bị. Lệnh Telnet được sử dụng để kiểm tra hoạt động phần mềm ở lớp ứng dụng giữa 2 máy.

- Telnet hoạt động ở lớp ứng dụng của mô hình OSI. Telnet hoạt động dựa trên cơ chế TCP để đảm bảo việc truyền dữ liệu giữa client và các server.

- Một router có thể cho phép thực hiện đồng thời nhiều phiên kết nối Telnet. Đường vty 0-4 trên router là đường dành cho Telnet. 5 đường Telnet này có thể thực hiện cùng lúc. Chúng ta cần lưu ý rằng việc sử dụng Telnet để kiểm tra kết nối lớp ứng dụng chỉ là việc phụ. Telnet được sử dụng chủ yếu để thiết lập kết nối từ xa vào thiết bị. Telnet là một chương trình ứng dụng đơn giản và thông dụng nhất.



Hình 4. 2: Telnet hoạt động ở lớp ứng dụng

2.2 Thiết lập và kiểm tra quá trình khởi động router

- Lệnh Telnet cho phép người dùng thực hiện Telnet từ một thiết bị Cisco này sang thiết bị khác. Chúng ta không cần phải nhập lệnh **connect** hay **telnet** để thiết lập kết nối Telnet mà chúng ta có thể nhập tên hoặc địa chỉ IP của router mà chúng ta muốn Telnet vào. Khi kết thúc phiên Telnet, dùng lệnh **exit** hoặc **logout**. Để thiết lập kết nối Telnet, dùng một trong các lệnh sau:

```
Denver>connect paris
```

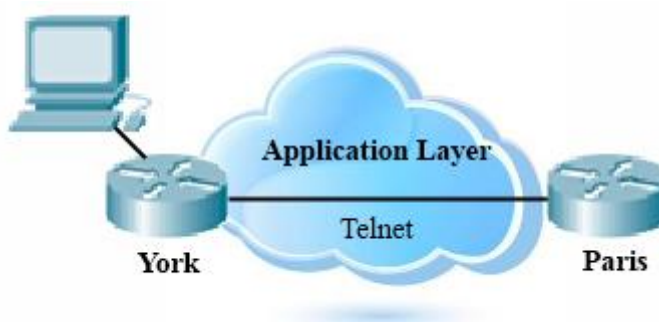
```
Denver>paris
```

```
Denver>131.108.100.12
```

```
Denver>telnet paris
```

- Router cần phải có bảng host hoặc là trong mạng phải có dịch vụ DNS phân giải tên máy mà chúng ta nhập vào. Nếu không thì bắt buộc phải dùng địa chỉ IP.

- Telnet được sử dụng để kiểm tra xem có thể kết nối từ xa vào một router hay không. Nếu có thể truy cập từ xa vào router thì có nghĩa là đã có ít nhất một ứng dụng TCP/IP kết nối vào được router đó. Một kết nối Telnet thành công chứng tỏ rằng các ứng dụng lớp trên hoạt động tốt.



Hình 4. 3: Telnet ở 2 vùng

2.3 Ngắt, tạm ngưng phiên Telnet

- Telnet có một đặc tính quan trọng là có thể tạm ngưng một phiên Telnet. Tuy nhiên có một rắc rối là khi sử dụng phím **enter** sau khi tạm ngưng phiên Telnet thì phần mềm Cisco IOS sẽ tự động quay trở lại kết nối Telnet vừa mới tạm ngưng trước đó. Mà phím **enter** là phím rất hay được sử dụng. Do đó khi tạm ngưng một phiên Telnet thì rất có thể sau đó sẽ kết nối lại vào một router khác. Điều này rất nguy hiểm khi thực hiện thay đổi cấu hình router. Do đó cần chú ý cẩn thận cấu hình của router trước khi tạm ngưng phiên Telnet trên router đó.

- Mỗi một phiên Telnet chỉ được tạm ngưng trong một khoảng thời gian giới hạn. Để quay trở lại kết nối Telnet mà đã tạm ngưng chỉ cần nhấn phím Enter. dùng lệnh **show session** để xem các kết nối Telnet đang được mở.

- Trình tự các bước để ngắt kết nối Telnet:

➤ **Bước 1:** Nhập lệnh **disconnect**.

- **Bước 2:** Tiếp theo sau lệnh này là tên hoặc địa chỉ IP của router.

Ví dụ: Denver> **disconnect paris**.

- Các bước thực hiện tạm ngưng phiên Telnet:

- **Bước 1:** Nhấn tổ hợp phím **Ctrl-Shift-6** cùng lúc, buông ra rồi nhấn tiếp chữ x.

- **Bước 2:** Nhập tên hoặc địa chỉ IP của router.

Initiate a session

```
Denver> telnet paris
```

End a session

```
Paris > exit
```

Suspend a session

```
Paris > <Ctrl><Shift><6><x>  
Denver >
```

Resume a session

```
Denver > <Return>
```

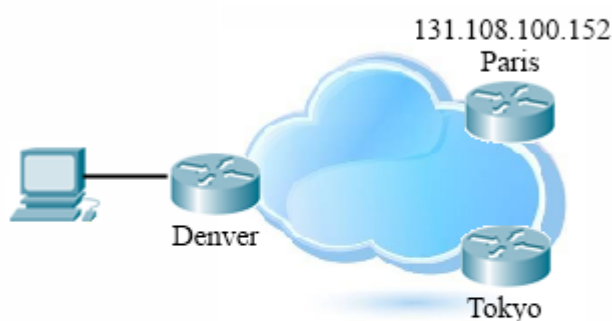
Disconnect a session

```
Denver> disconnect paris
```

Display Session

```
Denver #show sessions
```

Conn	Host	Address	Idle	Conn Name
1	Paris	131.108.100.152	0	Paris
2	Tokyo	126.102.57.63	0	Tokyo



Hình 4. 4: Trình tự Telnet

2.4 Mở rộng thêm về hoạt động Telnet

- Trên router có thể mở nhiều phiên Telnet cùng lúc. Chúng ta có thể chuyển đổi qua lại giữa các phiên Telnet này. có thể ấn định số lượng phiên Telnet được phép mở đồng thời trên router bằng lệnh **session limit**.

- Để chuyển đổi qua lại giữa các phiên Telnet, tạm ngưng phiên Telnet hiện tại và quay trở lại phiên mới mở trước đó.

- Nhấn tổ hợp phím **Ctrl-Shift-6** cùng lúc, buông ra rồi nhấn tiếp chữ x: tạm thoát khỏi kết nối hiện tại, quay lại dấu nhắc EXEC.

- Tại dấu nhắc EXEC, có thể thiết lập phiên kết nối mới. Router 2500 chỉ cho phép mở 5 phiên Telnet cùng lúc.

- có thể mở nhiều phiên Telnet cùng lúc và tạm ngưng bằng tổ hợp phím **Ctrl- Shift-6, x**. Nếu dùng phím Enter thì Cisco IOS sẽ tự động quay lại kết nối vừa mới tạm ngưng trước đó. Còn nếu dùng lệnh **resume** thì phải nhập thêm chỉ số ID bằng lệnh **show session**.

```

Denver>telnet Paris
Trying Paris (131.108.100.152)...Open
User Access Verification
Password: xxxx
Paris> (User pressed Ctrl-Shift-6, then x)
Denver>telnet Tokyo
Trying Tokyo (127.102.57.63)...Open
User Access Verification
Password: xxxxxx
Tokyo> (User pressed Ctrl-Shift-6, then x)
Denver> show sessions
Conn Host Address      Idle      Conn Name
  1  131.108.100.152      0         Paris
  2  127.102.57.63        0         Tokyo

```

Hình 4. 5: Tổ hợp phím Ctrl- Shift-6, x

2.5 Các lệnh kiểm tra kết nối khác

- Để hỗ trợ việc kiểm tra nối mạng cơ bản, nhiều giao thức mạng có hỗ trợ giao thức phản hồi (echo). Giao thức phản hồi được sử dụng để kiểm tra việc định tuyến các gói dữ liệu. Lệnh ping thực hiện gửi đi một gói dữ liệu tới máy đích và chờ nhận gói trả lời về từ máy đích. Kết quả của giao thức phản hồi giúp xác định độ tin cậy của đường truyền tới máy đích, thời gian trễ trên đường truyền, máy đích có đến được hay không, có hoạt động hay không. Lệnh ping là lệnh cơ bản để kiểm tra kết nối. Dùng lệnh này ở chế độ EXEC người dùng hay EXEC đặc quyền đều được.



```

Router> ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!
Seccess rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>

```

Hình 4. 6: :Lệnh kiểm tra kết nối

- Việc kiểm tra cơ bản cũng tập trung chủ yếu vào lớp Mạng. dùng lệnh **show ip route** để kiểm tra bảng định tuyến của router cho hệ thống mạng.
- Các bước thực hiện **ping**:
 - + **Bước 1**: Nhập lệnh ping, theo sau là địa chỉ IP hoặc tên của máy đích.
 - + **Bước 2**: Nhấn phím Enter.

- Các bước thực hiện lệnh **tracert**:

+ **Bước 1:** Nhập lệnh **tracert**, theo sau là địa chỉ IP hoặc tên của máy đích.

+ **Bước 2:** Nhấn phím Enter.

2.6 Xử lý sự cố về địa chỉ IP

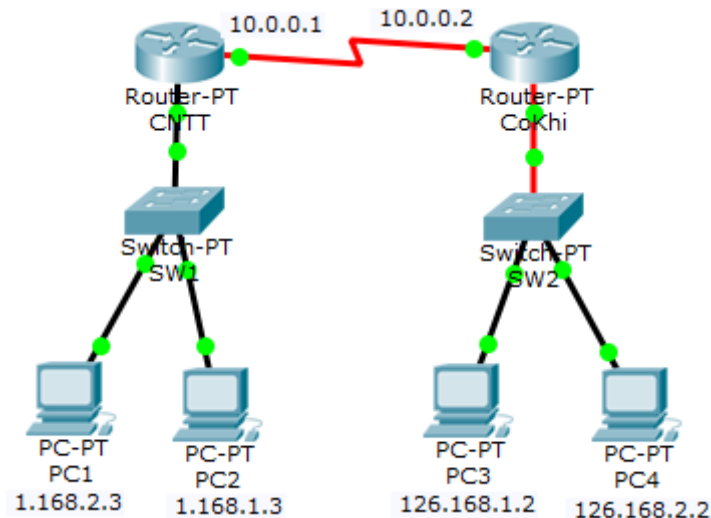
- Sự cố về địa chỉ là sự cố xảy ra phổ biến nhất trong mạng IP. Sau đây là 3 lệnh thường được sử dụng để xử lý các sự cố liên quan đến địa chỉ:

- **Ping:** sử dụng giao thức ICMP để kiểm tra kết nối vật lý và địa chỉ IP của lớp Mạng. Đây là lệnh kiểm tra cơ bản.
- **Telnet:** kiểm tra kết nối phần mềm lớp Ứng dụng giữa nguồn và máy đích. Đây là lệnh kiểm tra kết nối hoàn chỉnh.
- **Tracert:** cho phép xác định vị trí lỗi trên đường truyền từ máy nguồn đến máy đích. Lệnh trace sử dụng giá trị Time to Live để tạo thông điệp từ mỗi router trên đường truyền.

3. BÀI TẬP THỰC HÀNH 4.1

3.1. Mô hình

- Cho mô hình mạng như hình 4.7:



Hình 4. 7: Mô hình PC kết nối Router

3.2. Yêu cầu

- + Bật và tắt giao thức CDP trên Router CNTT.
- + Sử dụng lệnh **show ip route** để hiển thị thông tin các địa chỉ ip trên Router.
- + Sử dụng lệnh **show cdp neighbors** để hiển thị thông tin về các mạng kết nối trực tiếp vào Router.

3.3. Chuẩn bị:

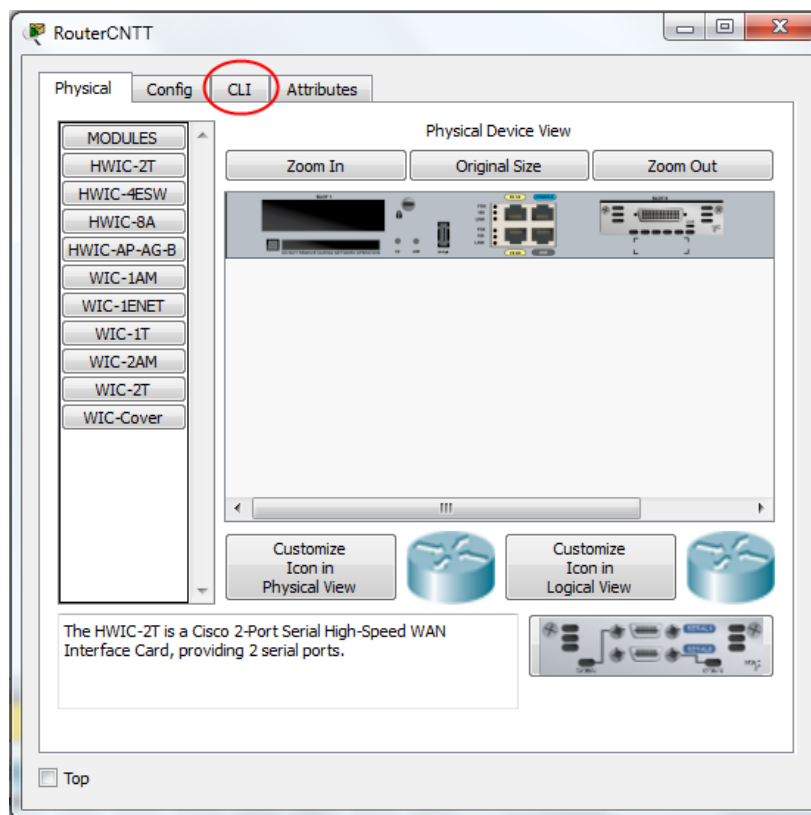
Bảng 4. 3: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 4.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	2	
2	Máy PC ảo	Máy	4	
3	Router ảo	Cái	2	
4	Switch	Cái	2	

3.4. Các bước thực hành:

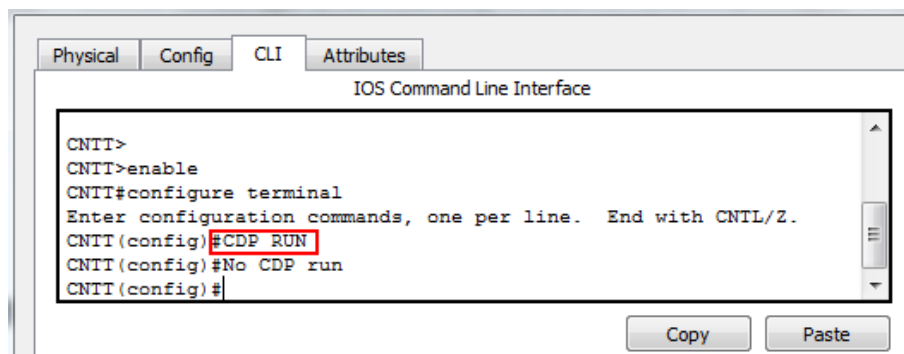
Bước 1: Bật giao thức CDP trên Router CNTT:

- Nhấn vào Router A trên mô hình như hình 4.8:



Hình 4. 8: Giao diện khi nhấn vào Router A

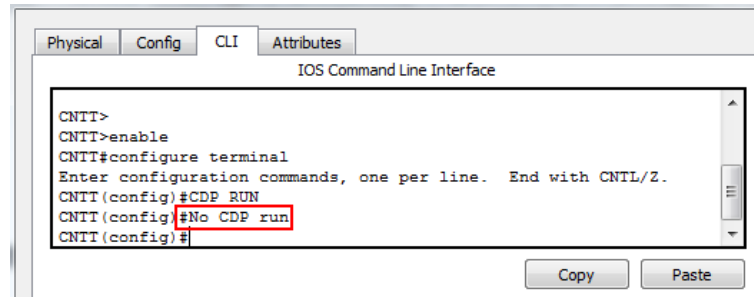
- Sau đó từ chế độ toàn cục ta gõ lệnh **cdp run**:



Hình 4. 9: Lệnh CDP run

Bước 2: Tắt giao thức CDP:

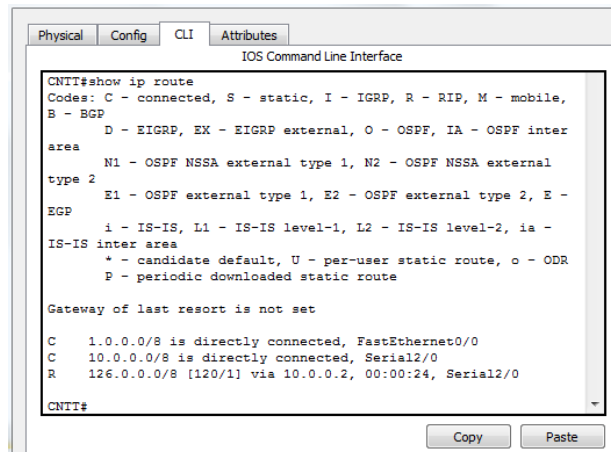
- Để tắt cdp, ta chuyển về chế độ toàn cục, rồi nhập lệnh **no cdp run**:



Hình 4. 10: Lệnh no CDP run

Bước 3: Hiển thị thông tin các địa chỉ ip trên Router CNTT

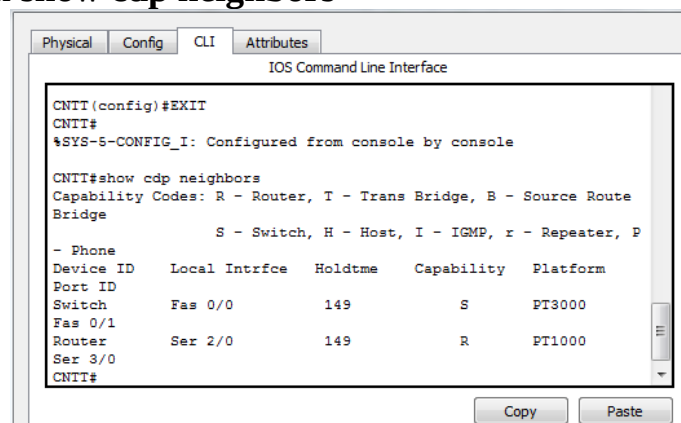
- Từ giao diện tab CLI, ta nhấn exit để vào chế độ EXEC đặt quyền,
- Sau đó gõ lệnh **show ip route**:



Hình 4. 11: Hiển thị thông tin địa chỉ ip trên Router

Bước 4: Hiển thị thông tin về các mạng kết nối trực tiếp vào Router:

- Vào giao diện CLI
- Nhấn exit để vào chế độ EXEC đặt quyền
- Ta gõ lệnh **show cdp neighbors**



Hình 4. 12: Hiển thị các mạng kết nối trực tiếp vào Router

3.5.Những sự cố thường gặp

Bảng 4. 4: những sự cố thường gặp của bài tập 4.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không bật giao thức CDP	Chọn sai router	Kiểm tra chọn lại đúng tên router
Không tắt giao thức CDP	Chọn sai chế độ dòng lệnh	Kiểm tra và chọn lại chế độ dòng lệnh
Không thông mạng	Do đặt sai địa chỉ IP	Kiểm tra và đặt lại địa chỉ IP
Ping thông mạng nhưng các thông tin trên router không đúng	Do nhập sai dòng lệnh	Kiểm tra và nhập lại dòng lệnh hiển thông tin

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7. Đánh giá các bước thực hành

Bảng 4. 5: đánh giá các bước thực hành bài tập 4.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Bật giao thức CDP trên Router CNTT	Chọn đúng router			
2	Bước 2: Tắt giao thức CDP	Chuyển đúng chế độ rồi mới tắt			
3	Bước 3: Hiển thị thông tin các địa chỉ ip trên Router CNTT	Chọn đúng chế độ đặt quyền			
4	Bước 4: Hiển thị thông tin về các	Nhập đúng dòng lệnh			

	mạng kết nối trực tiếp vào Router				
--	-----------------------------------	--	--	--	--

4.TÓM TẮT NỘI DUNG

- Thu nhập thông tin về các thiết bị láng giềng bằng cách sử dụng CDP.
- Thiết lập kết nối Telnet.
- Kết thúc kết nối Telnet.
- Tạm ngưng kết nối Telnet.
- Thực hiện kiểm tra kết nối.
- Xử lý sự cố của kết nối đầu cuối từ xa.

5.CÂU HỎI VÀ BÀI TẬP

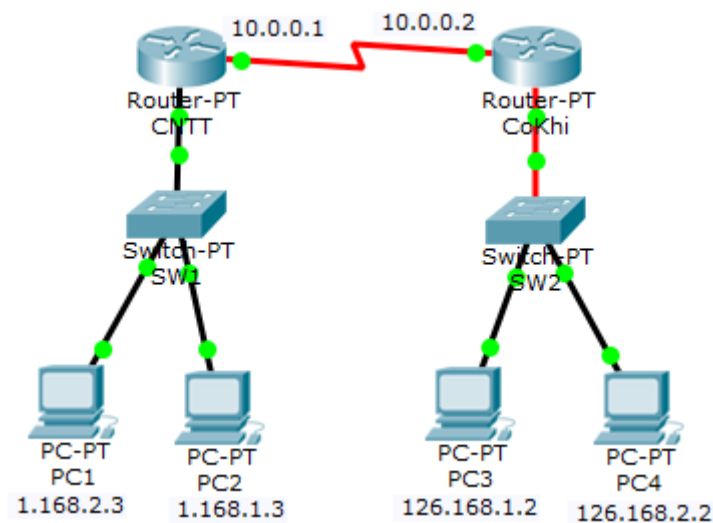
Câu hỏi:

Câu 1: Giao thức CDP là gì? Thông tin thu nhận được từ CDP?

Câu 2: Trình bày các câu lệnh xử lý sự cố của CDP và ý nghĩa của các câu lệnh?

Bài tập:

Cho mô hình mạng như hình :



- Cấu hình Telet cho từng Router.
- Cài đặt thời gian lưu giữ thông tin cho các gói CDP cập nhật được phát đi.
- Kiểm tra Cisco IOS hỗ trợ SSH, tạo key để sử dụng cho SSH và cấu hình enable tính năng SSH trên Router để quản trị từ xa.

BÀI 5:QUẢN LÝ PHẦN MỀM IOS

Mã bài MD 28-05

Thời gian: 8 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Xác định được router đang ở giai đoạn nào trong quá trình khởi động;
- Xác định giá trị thanh ghi cấu hình;
- Trình bày khái quát các tập tin IOS sử dụng;
- Sử dụng các lệnh Boot system;
- Nắm được nơi nào mà router lưu các loại tập tin khác nhau;
- Thực hiện các thao tác an toàn với máy tính;

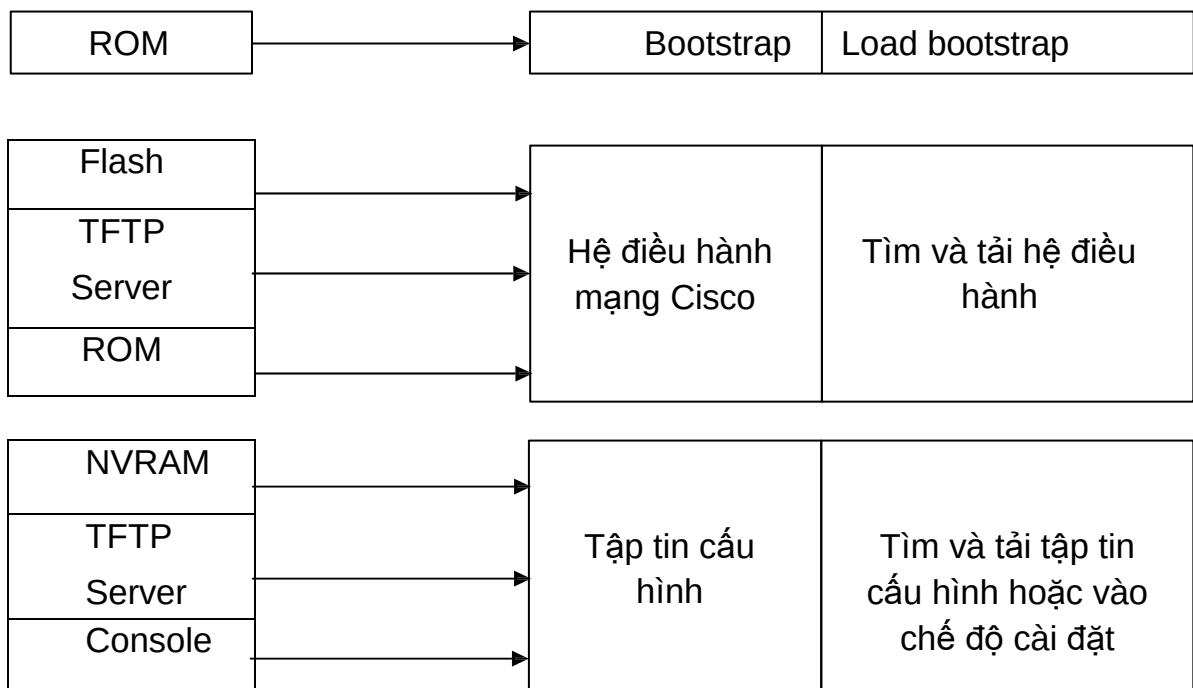
II.NỘI DUNG CHÍNH

1. Khảo sát và kiểm tra hoạt động router

1.1 Các giai đoạn khởi động router khi bắt đầu bật điện

- Mục tiêu chính của quá trình khởi động router là khởi động các hoạt động của router. Router phải hoạt động với độ tin cậy cao để thực hiện kết nối cho bất kỳ loại mạng nào. Do đó, quá trình khởi động router phải thực hiện các công việc như sau:

- + Kiểm tra phần cứng của router.
- + Tìm và tải phần mềm Cisco IOS.
- + Tìm và thực hiện các câu lệnh cấu hình, trong đó bao gồm các cấu hình giao thức và địa chỉ cho các cổng giao tiếp.



1.2 Thiết bị Cisco tìm và tải IOS như thế nào

- Nguồn mặc định tải phần mềm Cisco IOS thì khác nhau tùy theo phiên bản phần cứng của thiết bị, nhưng hầu hết các router đều tìm lệnh **boot system** lưu trong NVRAM. Phần mềm Cisco IOS có thể được tải từ nhiều nguồn khác nhau. Những nguồn này chúng ta có thể cấu hình hoặc router sẽ sử dụng quá trình tìm và tải phần mềm mặc định của nó.

- Giá trị cài đặt cho thanh ghi cấu hình sẽ cho phép router tìm IOS như sau:
 - + Lệnh **boot system** cấu hình cho router nơi mà router tìm để tải IOS. Router sẽ sử dụng các câu lệnh này theo thứ tự khi khởi động.
 - + Nếu trong NVRAM không có các câu lệnh **boot system** thì hệ thống sẽ mặc định là sử dụng Cisco IOS trong bộ nhớ flash.
 - + Nếu trong bộ nhớ flash cũng không có IOS thì router sẽ cố gắng sử dụng TFTP để tải IOS về. Router sẽ sử dụng giá trị cài đặt cấu hình để biết tên tập tin lưu trên server mạng.

1.3 Sử dụng lệnh boot system

Cài đặt thanh ghi cấu hình, lưu trong NVRAM, giá trị cài đặt cho thanh ghi cấu hình khác nhau sẽ cho phép router xác định vị trí tải IOS khác nhau.

```
Router# configure terminal
Router(config)# boot system flash IOS_filename
Router(config)# boot system tftp IOS_filename
tftp_address
Router(config)# boot system ROM
[Ctrl-Z]
Router# copy running-config startup-config
```

Không tìm thấy lệnh boot system trong NVRAM.

Bộ nhớ Flash không có IOS.

Tải Cisco IOS mặc định trong bộ nhớ Flash.

Tải Cisco IOS mặc định từ TFTP server.

1.4 Thanh ghi cấu hình

- Giá trị thanh ghi cấu hình không đúng cũng dẫn đến việc router không tải được IOS vì giá trị thanh ghi này sẽ cho router biết là tải IOS từ đâu. Chúng ta kiểm tra giá trị thanh ghi bằng lệnh **show version** và đọc dòng cuối cùng trong kết quả hiển thị của lệnh này. Giá trị thanh ghi cấu hình sẽ khác nhau đối với các biên bản phần cứng khác nhau. Có thể tham khảo giá trị thanh ghi cấu hình trên đĩa CD tài liệu của Cisco trên website của Cisco. Sau đó chỉnh sửa lại giá trị thanh ghi cấu hình rồi lưu vào tập tin cấu hình khởi động.

- Nếu sự cố vẫn tiếp tục xảy ra thì có thể là tập tin trong bộ nhớ flash bị lỗi. Thông thường, trong trường hợp như vậy sẽ gặp các thông báo lỗi trong quá trình khởi động router.

- Open: read error...requested 0x4 bytes, got 0x0
- Trouble reading device magic number
- Boot: cannot open "flash:"
- Boot: cannot determine first file name on device "flash:"

- Nếu dùng là tập tin trong flash bị lỗi thì cần chép lại IOS mới lên router.

1.5 Xử lý sự cố khi khởi động IOS

- Khi router không khởi động được thì có thể là do một trong những nguyên nhân sau:

- Mất tập tin cấu hình hoặc câu lệnh **boot system** bị sai.
- Giá trị thanh ghi cấu hình bị sai.
- Bộ nhớ flash bị trục trặc.
- Hư hỏng phần cứng.

- Khi router khởi động, router sẽ tìm câu lệnh **boot system** trong tập tin cấu hình. Lệnh **boot system** có thể cài đặt cho router khởi động từ IOS khác thay vì từ IOS trong flash. Để xác định xem router khởi động từ IOS nào, dùng lệnh **show version** và tìm dòng nói về phần mềm khởi động hệ thống.

- Sử dụng lệnh **show running-config** và tìm câu lệnh **boot system** nằm ở ngay phần đầu của tập tin cấu hình. Nếu câu lệnh **boot system** chỉ sai IOS thì chúng ta xoá lệnh đó đi bằng lệnh "no" của câu lệnh đó.

2. Quản lý tập tin hệ thống.

2.1 Khái quát về tập tin hệ thống IOS

- Hoạt động của router và switch phụ thuộc vào phần mềm cài trên nó. Có 2 loại phần mềm cần phải có để thiết bị hoạt động là: hệ điều hành và tập tin cấu hình.

- Hệ điều hành được sử dụng cho hầu hết các thiết bị Cisco là hệ điều hành liên mạng Cisco, gọi tắt là Cisco IOS (Internetwork Operating System).

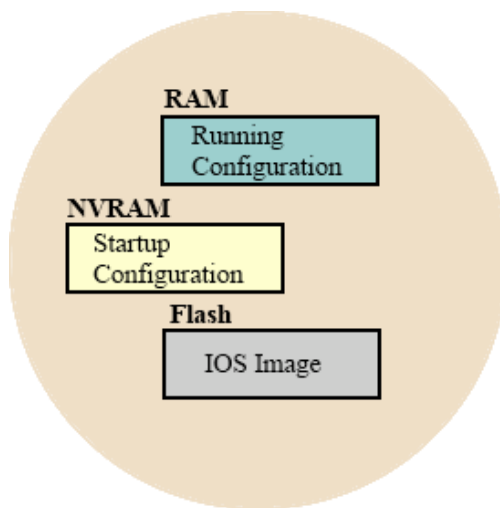
- Phần mềm Cisco IOS cho phép thiết bị thực hiện các chức năng của router hay switch. Một tập tin IOS khoảng vài megabyte.

- Phần mềm thứ 2 được sử dụng cho router và switch là tập tin cấu hình. Tập tin cấu hình chứa các hướng dẫn về hoạt động định tuyến hay chuyển mạch của thiết bị. Người quản trị mạng là người tạo tập tin cấu hình để các thiết bị Cisco thực hiện các chức năng theo đúng thiết kế của mình. Một số thông số mà có thể cấu hình được là địa chỉ IP của các cổng trên router, giao thức định tuyến và các mạng mà giao thức định tuyến đó được thực hiện quảng bá... Thông thường, một tập tin cấu hình từ vài trăm đến vài ngàn byte.

- Mỗi loại phần mềm được lưu thành từng tập tin riêng biệt trong từng bộ nhớ khác nhau.

- IOS được lưu trong loại bộ nhớ được gọi là flash. Flash lưu giữ ổn định tập tin IOS và tập tin IOS này được sử dụng để khởi động router. Flash cho phép chúng ta nâng cấp IOS và lưu được nhiều IOS khác nhau. Trong cấu trúc của một số loại router, IOS được copy lên RAM và chạy trên RAM.

- Tập tin cấu hình được lưu trong bộ nhớ NVRAM và tập tin này được sử dụng khi khởi động router. Do đó tập tin cấu hình được lưu trong NVRAM được gọi là tập tin cấu hình khởi động. Khi thiết bị khởi động, tập tin cấu hình khởi động được chép lên RAM. Khi đó tập tin này được chạy trên RAM và luôn được cập nhật khi đang chạy. Do đó tập tin đang chạy trên RAM được gọi là tập tin cấu hình hoạt động.



Hình 5. 1: tập tin hệ thống

- Bắt đầu từ phiên bản 12 của IOS, hệ thống tập tin Cisco IOS, gọi tắt là IFS (IOS File System), cung cấp một giao tiếp chung cho tất cả các hệ thống tập tin mà router đang sử dụng. IFS cung cấp một phương pháp chung để thực hiện quản lý toàn bộ hệ thống tập tin đang sử dụng cho router. Công việc này bao gồm tập tin trong bộ nhớ flash, hệ thống tập tin mạng (TFTP, rcp và FTP), đọc/viết dữ liệu (NVRAM, tập tin cấu hình hoạt động, ROM). IFS sử dụng các tiền tố để xác định hệ thống tập tin trên thiết bị.

2.2 Quy ước tên IOS

- Cisco phát triển rất nhiều phiên bản IOS khác nhau. Các phiên bản này hỗ trợ cho các phiên bản phần cứng với nhiều đặc tính khác nhau. Hiện nay Cisco vẫn đang tiếp tục phát triển nhiều phiên bản IOS mới.

- Để phân biệt giữa các phiên bản khác nhau, Cisco có một quy luật đặt tên cho IOS. Một tên của IOS bao gồm nhiều phần, mỗi phần thể hiện phiên bản phần cứng, các đặc tính hỗ trợ và số phát hành.

- **Phần đầu tiên** của tập tin IOS cho biết IOS này được thiết kế cho phiên bản phần cứng nào.

- **Phần thứ hai** của tên tập tin IOS cho biết tập tin này có hỗ trợ các đặc tính nào. Có rất nhiều đặc tính khác nhau để chọn lựa. Các đặc tính này được đóng gói trong Cisco IOS. Mỗi Cisco IOS chỉ có một số đặc tính chứ không có toàn bộ tất cả các đặc tính. Bên cạnh đó, các đặc tính này còn được phân loại như sau:

- + Cơ bản: các đặc tính dành cho từng phiên bản phần cứng, ví dụ: IP, IP/FW.
- + Mở rộng (Plus): là các đặc tính mở rộng hơn mức cơ bản, ví dụ IP Plus, IP/FW Plus, Enterprise Plus.
- + Mã hoá: vẫn là các đặc tính cơ bản hay mở rộng như trên nhưng có thêm 56 bit để mã hoá. Ví dụ: IP/ATM PLUS IPSEC 56, Plus 56, Enterprise Plus 56. Từ Cisco IOS phiên bản 12.2 trở đi, đặc tính mã hoá được thiết kế thành 2 loại là k8/k9:
 - K8: 64 bit mã hoa trở xuống.
 - K9: hơn 64 bit mã hoá.

- **Phần thứ 3** của tên tập tin cho biết định dạng của tập tin đó. Phần này cho biết IOS được lưu trong flash dưới dạng nén hay không, rồi IOS sẽ được giải nén để chạy ở đâu. Nếu IOS lưu trong flash dưới dạng nén thì nó sẽ được giải nén, chép lên RAM trong quá trình khởi động router. Dạng tập tin như vậy gọi là tập tin không cố định. Còn loại tập tin có định thì chạy trực tiếp trên flash luôn mà không cần chép lên RAM.

- **Phần thứ 4** của tập tin cho biết phiên bản của IOS. Phiên bản càng mới thì số trong phần này càng lớn.

2.3 Quản lý tập tin cấu hình bằng TFTP

- Trên Cisco router và switch, tập tin cấu hình hoạt động được để trên RAM và nơi cấu hình khởi động là NVRAM. Khi bị mất tập tin cấu hình thì ta phải có tập tin cấu hình khởi động dự phòng. Một trong những nơi mà chúng ta có thể lưu dự phòng tập tin cấu hình là TFTP server. Chúng ta dùng lệnh **copy running-config tftp** để chép tập tin cấu hình lên TFTP server. Sau đây là các bước thực hiện:

- Nhập lệnh **copy running-config tftp**.

- Ở dấu nhắc kế tiếp, nhập địa chỉ IP của TFTP server mà định lưu tập tin cấu hình.
- Đặt tên cho tập tin hoặc là lấy tên mặc định.
- Xác nhận lại các chọn lựa vừa rồi bằng cách gõ **yes**.
- Khôi phục lại cấu hình router bằng cách chép tập tin cấu hình đã lưu dự phòng trên TFTP server về router. Sau đây là các bước thực hiện
 - Nhập lệnh **copy running-config**.
 - Ở dấu nhắc kế tiếp, nhập địa chỉ IP của TFTP sever.
 - Kế tiếp, nhập tên của tập tin cấu hình mà mình muốn chép.
 - Xác nhận lại các chọn lựa rồi nhấn enter

2.4 Quản lý tập tin cấu hình bằng cách cắt-dán

- Một cách khác để tạo tập tin cấu hình dự phòng là chép lại kết quả hiển thị của lệnh **show running-config**. Từ thiết bị đầu cuối kết nối vào router, chúng ta chép lại kết quả hiển thị của lệnh **show running-config** rồi dán vào một tập tin văn bản sau đó lưu lại. Tuy nhiên tập tin văn bản này phải chỉnh sửa lại một chút trước khi chúng ta có thể sử dụng nó để khôi phục lại cấu hình router.

- Các bước thực hiện để chép lại tập tin cấu hình khi sử dụng Hyper Terminal:

- + **Bước 1:**Chọn **Transfer**.
- + **Bước 2:**Chọn **Capture Text**.
- + **Bước 3:**Đặt tên cho tập tin văn bản mà chúng ta sẽ chép tập tin cấu hình ra.
- + **Bước 4:**Chọn Start để bắt đầu quá trình chép.
- + **Bước 5:**Chọn hiển thị nội dung của tập tin cấu hình bằng lệnh **show running-config**.
- + **Bước 6:**Nhấn phím **space bar** mỗi khi có dấu nhắc "--More--" xuất hiện.
- + **Bước 7:**Sau khi tập tin cấu hình đã hiển thị đầy đủ, kết thúc quá trình chép.
- + **Bước 8:**Chọn **Transfer**.
- + **Bước 9:**Chọn **Capture**.
- + **Bước 10:**Chọn **Stop**.

- Sau khi quá trình chép hoàn tất, cần xoá bớt một số hàng trong tập tin cấu hình để sau này chúng ta có thể sử dụng tập tin văn bản này "dán" lại vào router. Ngoài ra, có thể thêm một số hàng chú thích vào tập tin cấu hình. Các hàng chú thích này được bắt đầu bằng dấu chấm than (!) ở đầu hàng.

- có thể sử dụng Notepad để chỉnh sửa tập tin cấu hình. ở Notepad, chọn **File>Open**. Chọn tên của tập tin cấu hình mà vừa chép được. Nhấn phím **Open**.

- Sau đây là những hàng trong tập tin cấu hình mà cần xoá:

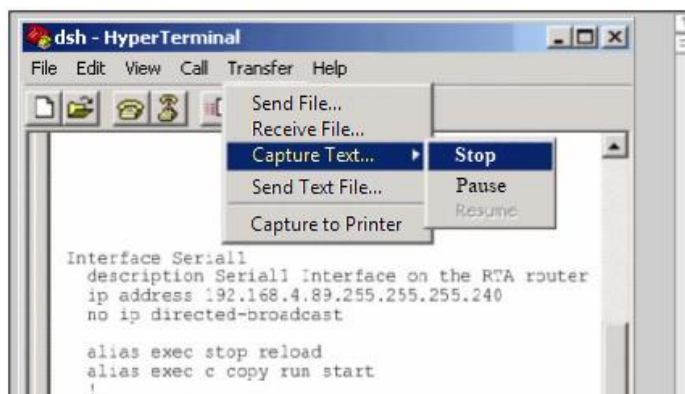
- Show running-config
- Building configuration...
- Current configuration:
- -More-
- Bất kỳ hàng nào ở sau dòng “End”

- thêm lệnh **no shutdown** vào cuối mỗi phần cấu hình của các cổng giao tiếp. Sau đó chọn **File>Save** để lưu lại tập tin cấu hình.

- Sau này, từ kết nối bằng HyperTerminal có thể khôi phục lại tập tin cấu hình cho router. Trước tiên, phải xoá hết tập tin cấu hình đang có trong router bằng lệnh **erase startup-config** ở chế độ EXEC đặc quyền. Sau đó khởi động lại router bằng lệnh **reload**.

- Các bước thực hiện để chép lại tập tin cấu hình cho router từ kết nối HyperTerminal:

- + **Bước 1:**Chuyển vào chế độ cấu hình toàn cục.
- + **Bước 2:**Trên HyperTerminal chọn **Transfer>Send Text File**.
- + **Bước 3:**Chọn tên của tập tin cấu hình mà cần chép lên router.
- + **Bước 4:**Từng dòng trong tập tin cấu hình sẽ được nhập vào y như lúc gõ lệnh đó vậy.
- + **Bước 5:**Theo dõi quá trình chép để xem có xảy ra lỗi gì hay không.
- + **Bước 6:**Sau khi tập tin cấu hình đã được chép xong, nhấn Ctrl-Z để thoát khỏi chế độ cấu hình toàn cục.
- + **Bước 7:**Lưu lại thành tập tin cấu hình khởi động bằng lệnh **copy running-config startup-config**.



Hình 5. 2: Quá trình chép tập tin bằng kết nối HyperTerminal

```

GAD#configure terminal
Enter configuraton commands, one per line. End with
CNTL/Z.
GAD(config)#
GAD(config)#service timestamps debug uptime
GAD(config)#service timestamps log uptime
GAD(config)#no service password-encryption
GAD(config)#!
GAD(config)#hostname GAD
.....
GAD(config-line)#line aux0
GAD(config-line)#line vty0 4
GAD(config-line)#password cisco
GAD(config-line)#login
GAD(config-line)#!
GAD(config-line)#end
GAD#copy running-config startup-config

```

Hình 5. 3: Quá trình chép tập tin cấu hình vào router bằng kết nối HyperTerminal

2.5 Quản lý Cisco IOS bằng TFTP

- Thỉnh thoảng router cũng cần lưu dự phòng hoặc nâng cấp IOS. Đầu tiên sau khi mua router, chúng ta cần lưu lại IOS để dự phòng. Có thể đặt IOS này trên một server trung tâm chung với các IOS khác. Các IOS này được sử dụng để thay thế hay nâng cấp cho các router, switch trong hệ thống mạng.

- Server phải có chạy dịch vụ TFTP và chúng ta chép IOS từ server lên router bằng lệnh **copy tftp flash** ở chế độ EXEC đặc quyền.

- Sau khi nhập lệnh trên, router sẽ hiển thị dấu nhắc yêu cầu nhập địa chỉ IP của TFTP server. Sau đó router sẽ yêu cầu xóa flash. Router thường yêu cầu xóa flash khi bộ nhớ flash không còn đủ chỗ trống để lưu thêm IOS mới. Router sẽ hiển thị một chuỗi các chữ “e” trong suốt quá trình xóa flash.

- Sau khi xóa xong flash, router bắt đầu tải IOS mới về. Router sẽ hiển thị một chuỗi các dấu chấm than (!) trong suốt quá trình chép. Một IOS có thể lớn khoảng vài Megabyte nên quá trình này cũng sẽ tốn một khoảng thời gian.

- Sau khi chép xong, router sẽ kiểm tra lại IOS mới trong flash. Sau khi kiểm tra hoàn tất thì lúc này router đã sẵn sàng cho khởi động lại để sử dụng IOS mới.

```

GAD#copy tftp flash
Address of remote host []? 192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-JS-L_121-3.bin]?
Accessing tftp://192.168.119.20/C2600-js-l_121-3.bin
Brace flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeeee.....eeeeeeeeeeeeeeee.....erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying Check sum.....OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#

```

Hình 5. 4: Lệnh copy tftp flash

2.6 Quản lý IOS bằng Xmodem

- Khi khởi động router mà IOS lưu trong flash bị xoá mất hoặc bị lỗi thì phải khôi phục lại IOS từ chế độ ROM monitor (ROMmon). Ở nhiều thiết bị Cisco, chế độ ROMmon được hiển thị bởi dấu nhắc rommon 1>.

- Bước đầu tiên cần phải xác định xem tại sao router không tải được IOS từ flash. Nguyên nhân là do mất IOS hay IOS bị lỗi. kiểm tra flash bằng lệnh **dir flash**:

- Nếu trong flash vẫn có một IOS bình thường thì thử khởi động router bằng IOS này bằng lệnh **boot flash:**. Ví dụ: nếu trong flash có rommon 1>**boot flash:c2600-is-mz.121-5**.

- Nếu router khởi động bình thường thì có 2 vấn đề cần kiểm tra xem tại sao router lại khởi động vào chế độ ROMmon mà không khởi động từ IOS trong flash. Đầu tiên, dùng lệnh **show version** để kiểm tra giá trị của thanh ghi cấu hình xem có đúng giá trị mặc định hay không. Nếu giá trị thanh ghi cấu hình đúng thì dùng lệnh **show startup-config** để xem có lệnh **boot system** nào cấu hình cho router khởi động vào chế độ ROM monitor hay không. flash thì cần phải chép một IOS mới. Từ chế độ ROMmon, có thể chép tập tin IOS bằng Xmodem qua đường console hoặc bằng TFTP.

- Chép IOS bằng Xmodem từ chế độ ROMmon.

- Trước tiên, cần phải có tập tin IOS trên máy tính như HyperTerminal chẳng hạn. có thể chép IOS với tốc độ mặc định của đường console là 9600, hoặc là có thể nâng tốc độ lên 115200. Trong chế độ ROMmon, dùng lệnh **confreg**, router sẽ hiển thị các giá trị mà có thể thay đổi được.

- Sau đó sẽ gặp câu hỏi “change console baud rate? y/n [n];”, nhập chữ y để xác nhận tốc độ mới. Sau khi thay đổi tốc độ đường console và khởi động lại router vào chế độ ROMmon, nên kết thúc phiên kết nối cũ (tốc độ 9600) và thiết lập lại phiên kết nối HyperTerminal mới với tốc độ mới là 115200 bit/s.

```
rommon 1 >confreg

Configuration Summary
...<output omitted>...
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n [n]: y
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7
change the boot characteristics? y/n [n]:

Configuration Summany
```

Hình 5. 5: Lệnh confreg

- Bây giờ dùng lệnh **xmodem** để chép phần mềm IOS từ PC. Cấu trúc câu lệnh này như sau: **xmodem -c image_file_name**. Ví dụ: chép IOS có tên

là “c2600-is-mz.122-10a.bin” thì gõ lệnh như sau:

Xmodem –c c2600-i-mz.122-10a.bin

- Tham số -c là để cho quá trình Xmodem sử dụng CRC (Cyclic Redundancy Check) kiểm tra lỗi trong suốt quá trình chép.
- Sau đó router sẽ hiển thị một dòng thông báo chưa bắt đầu quá trình chép và một thông điệp cảnh báo. Thông điệp này cảnh báo là nội dung bộ nhớ flash sẽ bị mất nếu chúng ta tiếp tục quá trình này và yêu cầu chúng ta xác nhận có tiếp tục hay không. Nếu chúng ta xác nhận cho tiếp tục thì router sẽ bắt đầu thực hiện chép IOS.

```
rommon 1 >
rommon 1 > xmodem -?
xmodem: illegal option -- ?
usage: xmodem [-cyrx] <destination filename>
        -c CRC-16
        -y ymodem-batch protocol
        -r copy image to dram for launch
        -x do not launch on download completion
rommon 2 > xmodem -c c2600-is-mz.122-10a.bin

Do not start the sending program yet...

Warning: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n In1: y
Ready to receive file c2600-is-mz.122-10e.bin...
```

Hình 5. 6: Lệnh Xmodem

- Lúc này cần cho bắt đầu quá trình Xmodem từ chương trình giả lập đầu cuối. Trong HyperTerminal chọn **Transfer>Send File**. Trong cửa sổ của **Send File**: chọn tên và vị trí lưu tập tin IOS, chọn giao thức là Xmodem, rồi bắt đầu quá trình truyền. Trong suốt quá trình truyền, cửa sổ Send File sẽ hiển thị trạng thái truyền.

- Khi quá trình truyền hoàn tất, sẽ gặp một thông điệp cho biết là bộ nhớ flash đang bị xoá, sau đó IOS được chép vào flash. Cuối cùng gặp thông điệp “Download Complete!”. Trước khi khởi động lại router, cần phải cài đặt lại tốc độ đường console là 9600 và đặt lại giá trị thanh ghi cấu hình là 0x2102 bằng lệnh:

config-register 0x2102.

- Trong lúc router đang khởi động lại thì nên kết thúc phiên kết nối 115200 và thiết lập lại phiên kết nối mới với tốc độ 9600.

2.7 Biến môi trường

- có thể khôi phục IOS bằng TFTP. Chép IOS bằng TFTP trong chế độ ROMmon là cách nhanh nhất để khôi phục IOS cho router. Để thực hiện cách này, cài đặt biến môi trường rồi dùng lệnh **tftpdnld**.

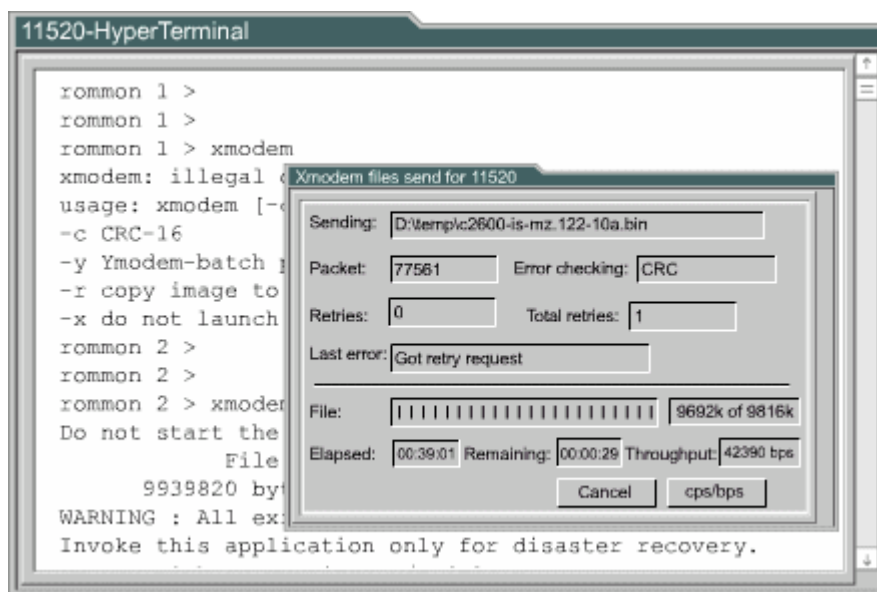
- Chế độ ROMmon có chức năng rất giới hạn vì chưa tải được tập tin cấu hình khi khởi động router. Do đó router không hề có IP hay cấu hình cho cổng giao tiếp nào. Các biến môi trường sẽ cung cấp cho router một cấu hình tối thiểu cho phép chạy TFTP để chép IOS. TFTP trong chế độ ROMmon chỉ hoạt động được với cổng LAN đầu tiên trên router, do đó cần cài đặt các đặc tính IP cho cổng LAN này. Để cài đặt giá trị cho các biến môi trường, đầu tiên nhập tên biến, tiếp theo là dấu bằng (=) rồi đến giá trị cài đặt cho biến đó (TÊN BIẾN = giá trị cài đặt). Ví dụ: muốn đặt địa chỉ IP là 10.0.0.1 thì ở dấu nhắc của chế độ ROMmon nhập câu lệnh là:

IP_ADDRESS=10.0.0.1

- Sau đây là các biến tối thiểu mà cần phải đặt để sử dụng cho lệnh **tftpdnld**:

- IP_ADDRESS: địa chỉ IP cho cổng LAN.
- IP_SUBNET_MASK: subnet mask cho cổng LAN.
- DEFAULT_GATEWAY: đường mặc định cho cổng LAN.
- TFTP_SERVER: địa chỉ IP của TFTP server.
- TFTP_FILE: tên tập tin IOS lưu trên server.

- Để kiểm tra lại giá trị của các biến môi trường, dùng lệnh **set**.



Hình 5. 7: Cửa sổ Send File

- Sau khi cài đặt xong các biến môi trường, nhập lệnh **tftpdnld**, không có tham số nào tiếp theo hết. Router sẽ hiển thị lại giá trị các biến, theo sau là thông điệp cảnh báo quá trình này sẽ xóa flash và yêu cầu chúng ta xác nhận có cho tiếp tục quá trình này hay không.

- Trong quá trình chép, router hiển thị dấu chấm than (!) cho biết đã nhận được các gói dữ liệu. Sau khi nhận xong tập tin IOS, router bắt đầu xóa flash rồi chép tập tin IOS mới vào flash. sẽ gặp một thông báo khi quá trình này hoàn tất.

- Sau đó, từ dấu nhắc của chế độ ROMmon, có thể khởi động lại router bằng cách nhập chữ **i**. Router sẽ khởi động lại với IOS mới trong flash.

2.8 Kiểm tra tập tin hệ thống

- Có rất nhiều lệnh để kiểm tra tập tin hệ thống của router. Trong đó có thể sử dụng lệnh **show version**. Lệnh **show version** có thể kiểm tra được tập tin hiện tại trong flash và tổng dung lượng của bộ nhớ flash. Ngoài ra lệnh này còn cung cấp thêm một số thông tin về lần tải IOS gần nhất như: trong lần khởi động gần nhất, router tải IOS nào, từ đâu; giá trị thanh ghi cấu hình hiện tại là bao nhiêu. Nếu vị trí mà router tải IOS trong flash đã bị mất hoặc bị lỗi, hoặc là có lệnh boot system trong tập tin cấu hình khởi động.

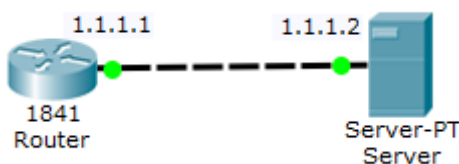
- Bên cạnh đó, có thể dùng lệnh **show flash** để kiểm tra tập tin hệ thống. Lệnh này kiểm tra được trong flash hiện đang có tập tin IOS nào, tổng dung lượng flash còn trống là bao nhiêu. Chúng ta thường dùng lệnh này để xem bộ nhớ flash có đủ dung lượng cho IOS mới hay không.

- Như các phần trên đã đề cập, tập tin cấu hình có thể có các lệnh boot system. Lệnh boot system xác định cho router vị trí tải IOS khi khởi động. Chúng ta có thể cấu hình nhiều lệnh boot system và router sẽ thực thi theo thứ tự các câu lệnh này trong tập tin cấu hình.

3.BÀI TẬP THỰC HÀNH 5.1

3.1.Mô hình

- Cho mô hình mạng như hình 5.7:



Hình 5. 8: Mô hình Router kết nối Server

3.2.Yêu cầu:

Cập nhật phần mềm IOS cho Router 1841 trên phần mềm Cisco Packet Tracer.

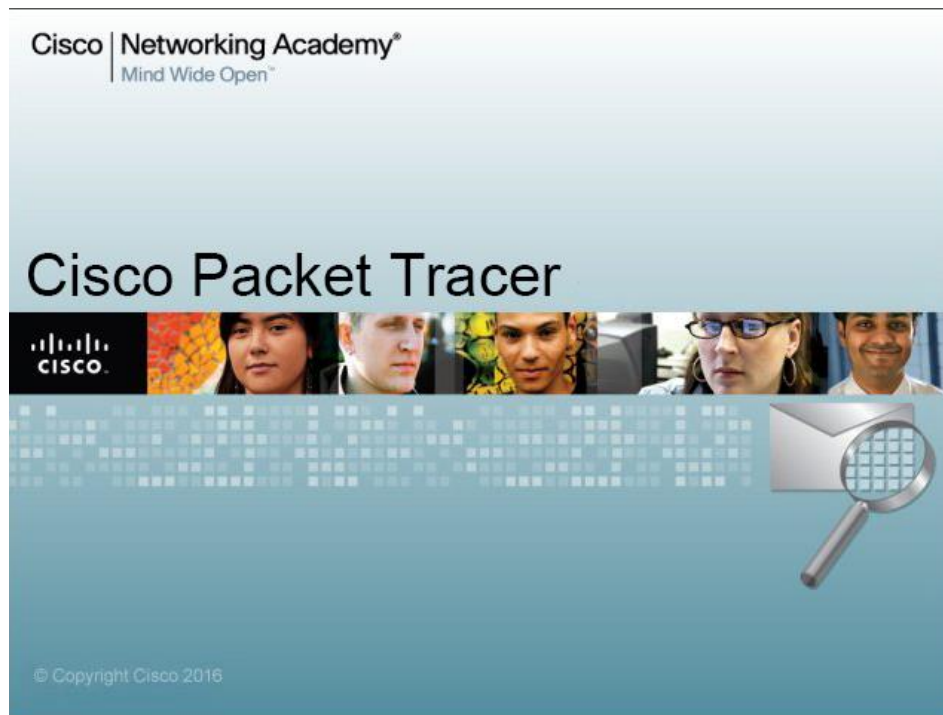
3.3.Chuẩn bị:

Bảng 5. 1: chuẩn bị phần cài đặt, máy tính, router thực hành bài tập 5.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	1	
3	Router ảo	Cái	1	

3.4.Các bước thực hành:

Bước 1: Khởi động phần mềm Cisco Packet Tracer.



Hình 5. 9: Khởi động phần mềm Cisco Packet Tracer

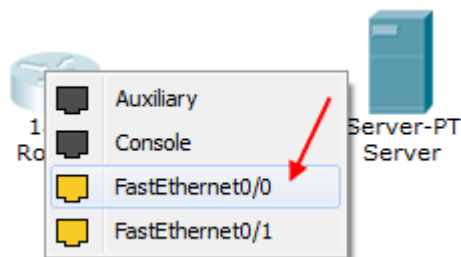
Bước 2: Chọn thiết bị cấu hình như mô hình:



Hình 5. 10: Chọn thiết bị Router và Server

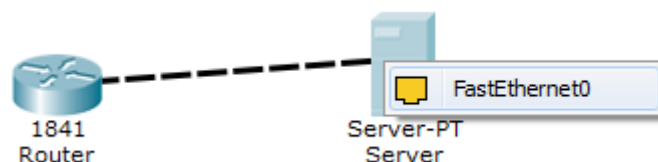
Bước 3: Kết nối Router và Server:

- Chọn cổng FastEthernet0/0 cho Server



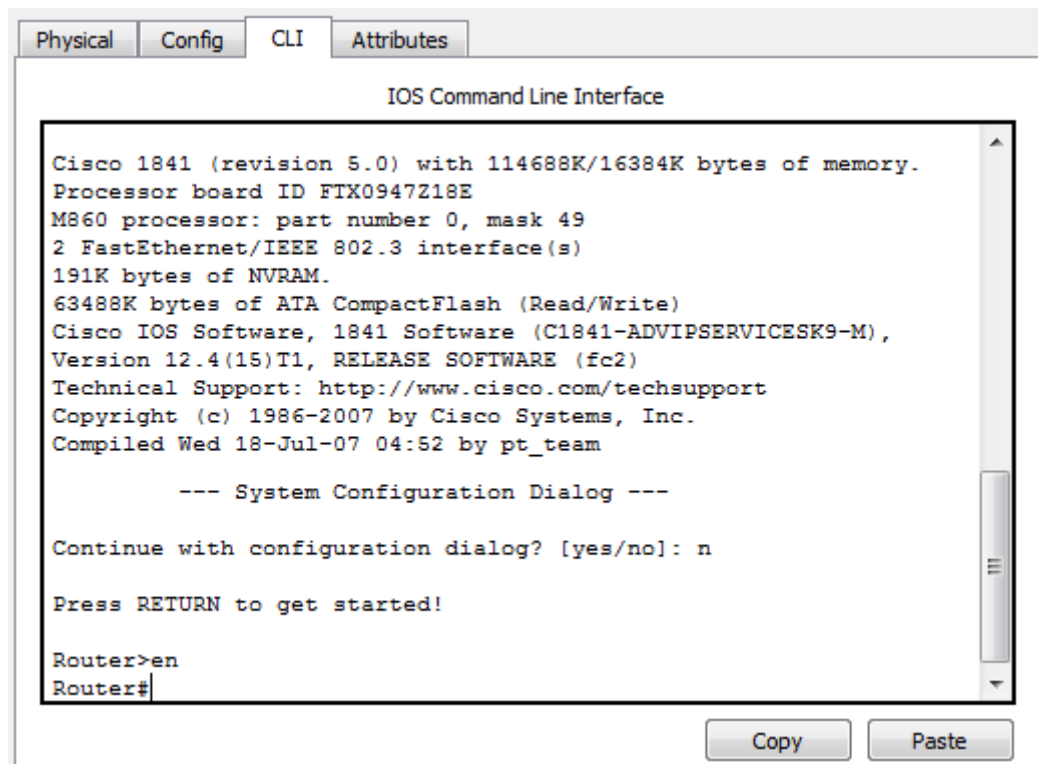
Hình 5. 11: Chọn cổng FastEthernet0/0

- Chọn cổng FastEthernet0 cho Router



Hình 5. 12: Chọn cổng FastEthernet0

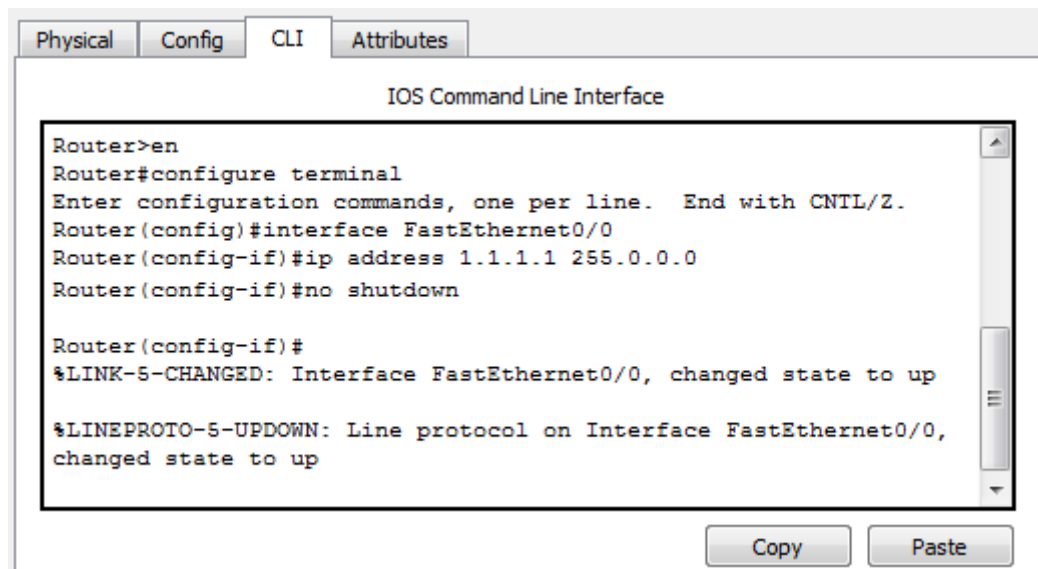
Bước 4: Vào Router sau đó chuyển sang Tab CLI sau đó gõ lệnh Enable để chuyển sang chế độ đặt quyền



Hình 5. 13: Chuyển sang chế độ đặt quyền

Bước 5: Cấu hình địa chỉ IP và Subnet Mask cho Router:

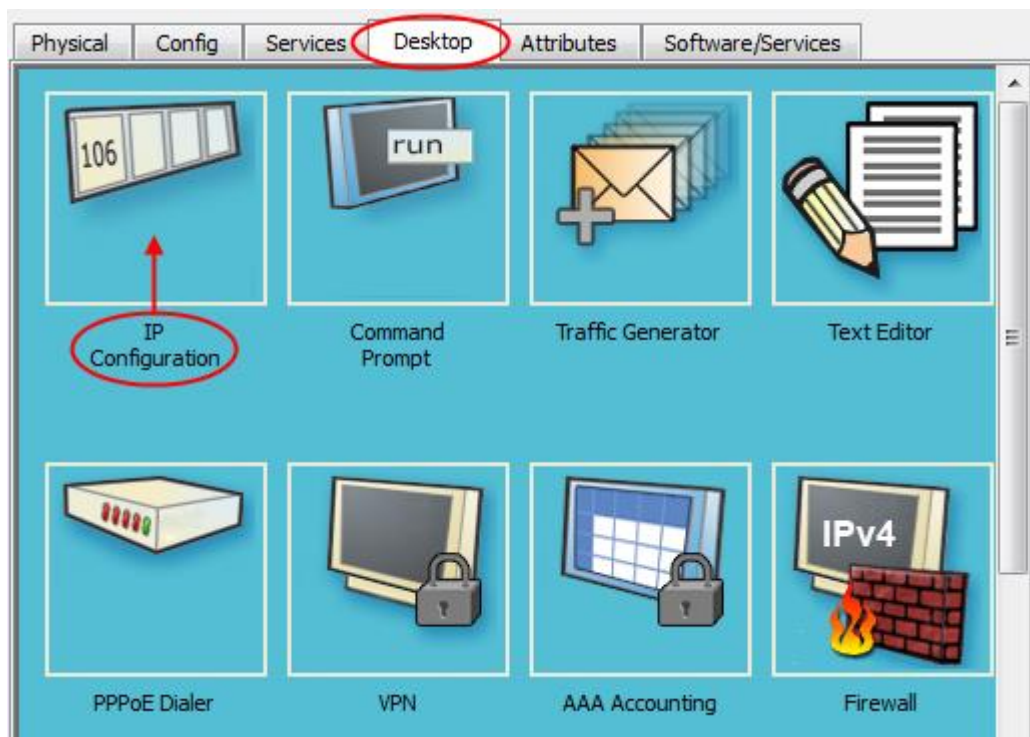
- Ta gõ lệnh **interface [cổng FastEthernet0/0]**
- Sau đó khai báo địa chỉ IP và subnet mask bằng lệnh **ip address <địa chỉ ip> <subnet mask>**
- Gõ tiếp lệnh **no shutdown** để khởi động cổng FastEthernet0/0



Hình 5. 14: Cấu hình địa chỉ IP và Subnet Mask cho Router

Bước 6: Cấu hình cho Server:

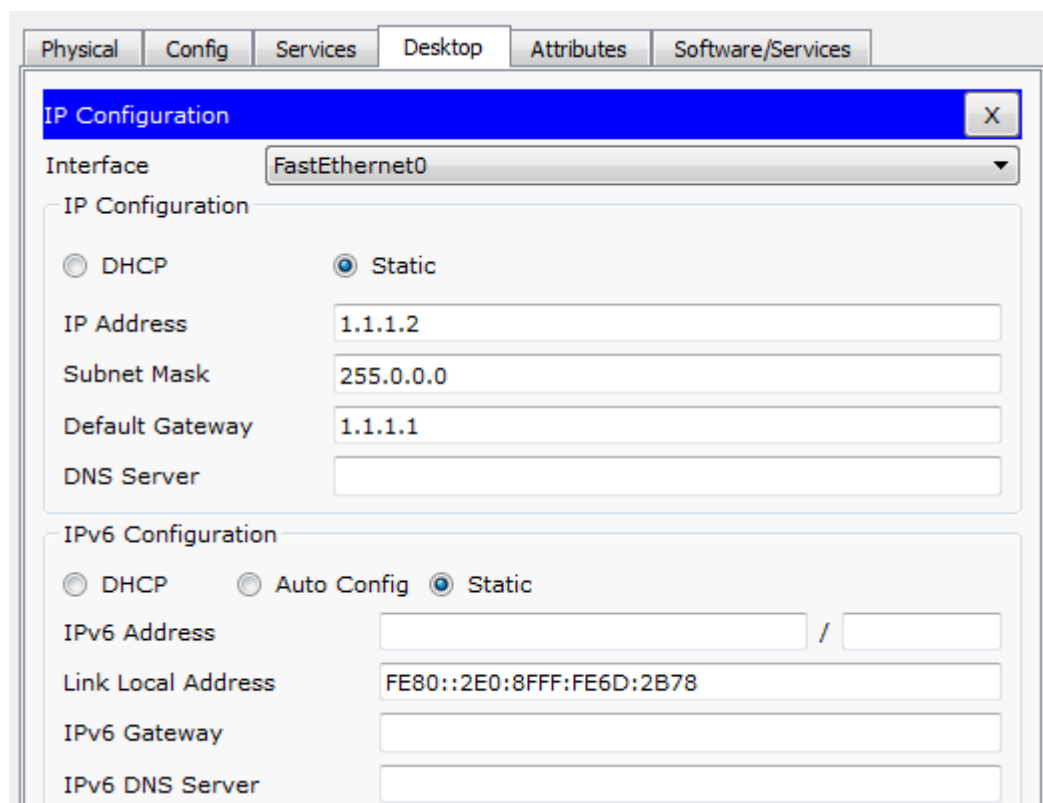
- Vào Server chuyển sang tab **Desktop** rồi chọn **IP Configuration:**



Hình 5. 15: Chọn IP Configuration

Bước 7: Nhập địa chỉ IP và Subnet Mask cho Server

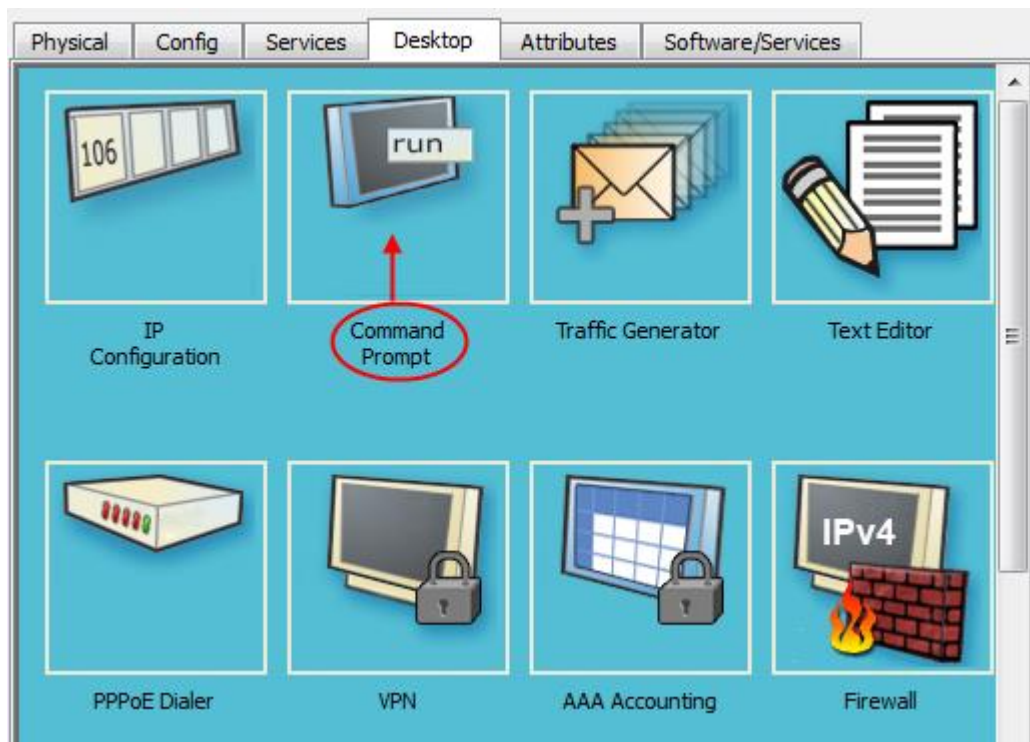
- Nhập địa chỉ IP, Subnet và Default Gateway như hình 5.15:



Hình 5. 16: Nhập địa chỉ IP, Subnet và Default Gateway cho Server

Bước 8: Ping Server qua Router:

- Trở về tab **Desktop** và chọn **Command Prompt**



Hình 5. 17: Chọn Command Prompt

- Sau đó gõ lệnh **Ping [địa chỉ IP Router]**
- Kết quả hiện ra 4 dòng Reply from 1.1.1.1 ... TTL=255 là Ping thành công.

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time=17ms TTL=255
Reply from 1.1.1.1: bytes=32 time<1ms TTL=255
Reply from 1.1.1.1: bytes=32 time<1ms TTL=255
Reply from 1.1.1.1: bytes=32 time<1ms TTL=255

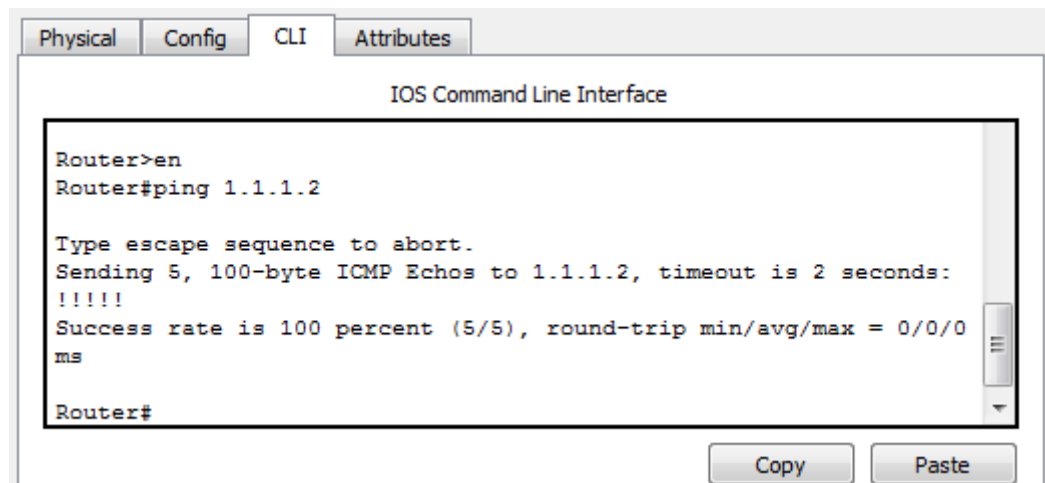
Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>|
```

Hình 5. 18: Ping Server qua Router

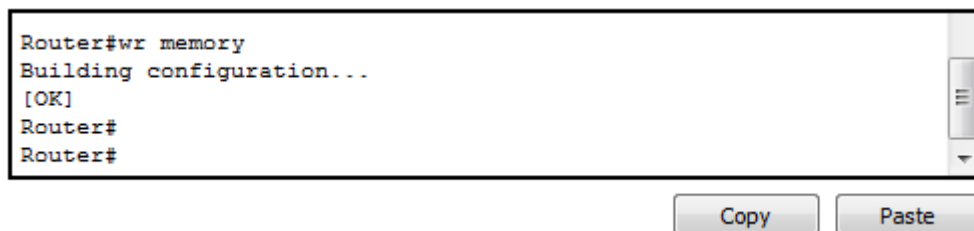
Bước 9: Ping Router qua Server:

- Từ tab CLI ta gõ lệnh **ping [địa chỉ IP Server]**
- Xuất hiện dòng **Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms** là ping thành công.



Hình 5. 19: Ping Router qua Server

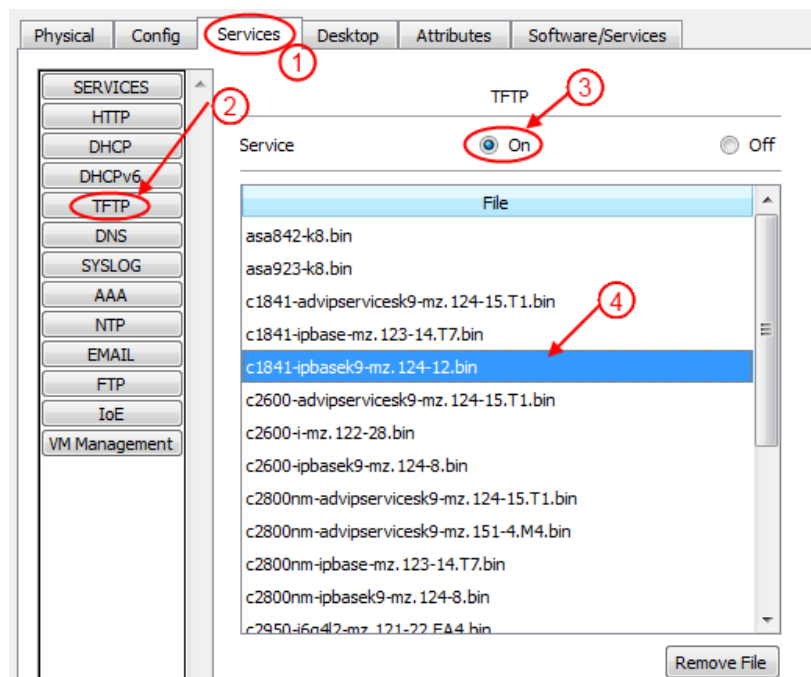
Bước 10: Gõ lệnh **write memory** để lưu file cấu hình từ DRAM vào NVRAM



Hình 5. 20: : Lưu file cấu hình từ DRAM vào NVRAM

Bước 11: Bật dịch vụ TFTP trên máy chủ TFTP Server.

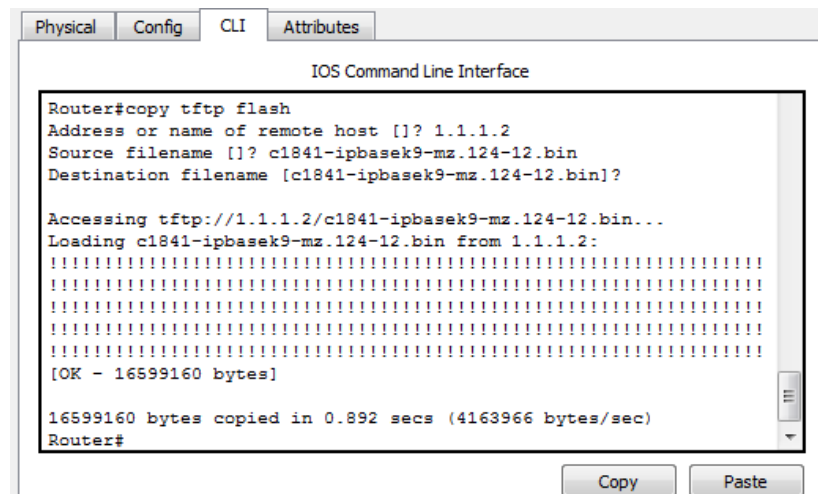
- Vào Sever chọn tab Services
- Chọn TFTP và tích chọn On
- Chọn và copy dòng **c1841-ipbasek9-mz.124-12.bin**



Hình 5. 21: Bật dịch vụ TFTP trên máy chủ TFTP Server

Bước 12: Copy IOS image mới vào bộ nhớ Flash của Router

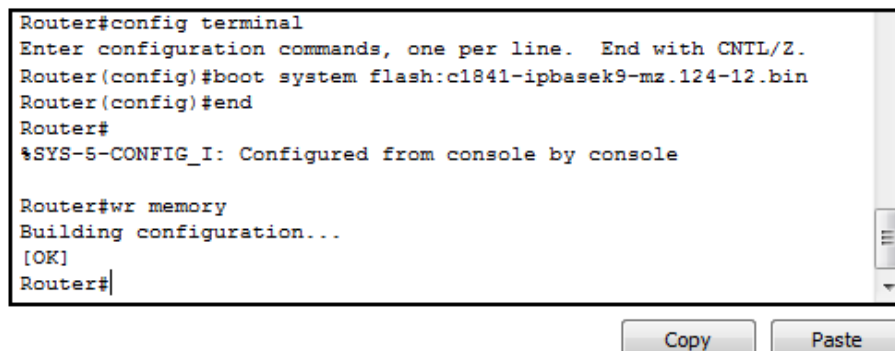
- Gõ lệnh **copy tftp flash**
- Nhập địa chỉ Ip máy chủ Server
- Dán source filename đã copy sau đó enter



Hình 5. 22: Copy IOS image mới vào bộ nhớ Flash của Router

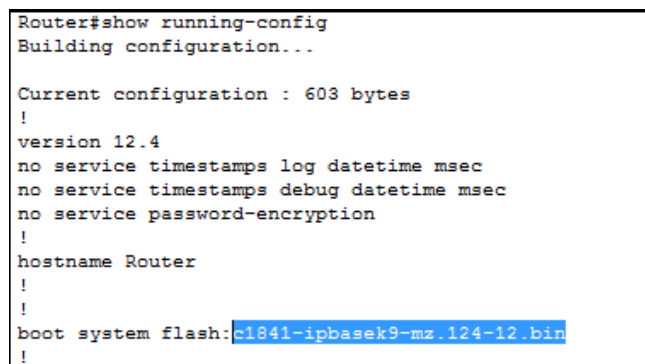
Bước 13: Đặt biến khởi động cho Router và ghi cấu hình:

- Gõ lệnh **boot system flash: [filename]** để cài boot variable trong Router.
- Sau đó gõ lệnh **end** và **wr memory** để lưu lại vào bộ nhớ NVRAM.



Hình 5. 23: Đặt biến khởi động cho Router và ghi cấu hình

- Kiểm tra lại bằng cách gõ lệnh **show running-config**
- Ta sẽ thấy dòng **boot system flash:c1841-ipbasek9-mz.124-12.bin**



Hình 5. 24: : Kiểm tra bằng lệnh show running-config

Bước 14: Reload lại Router bằng cách sử dụng lệnh **reload**

```

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Initializing memory for ECC
--
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

Self decompressing the image :
#####

```

Hình 5. 25: Tải lại Router

Bước 15: Sau khi Reload, kiểm tra lại **system image file name** bằng lệnh **show version**:

- Ta sẽ thấy dòng **System image file is "flash:c1841-ipbasek9-mz.124-12.bin"** đó là IOS image mới.

```

Router#show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version
12.4(12), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbasek9-mz.124-12.bin"

This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this
product you
agree to comply with applicable laws and regulations. If you are
unable

```

Hình 5. 26: Kiểm tra lại system image file name IOS mới

3.5.Những sự cố thường gặp

Bảng 5. 2: những sự cố thường gặp của bài tài tập 5.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không kết nối được PC với router	Chọn sai cổng kết nối	Chọn đúng cổng và bật chế độ mở
Không nhập được địa chỉ IP	Chọn sai máy server	Chọn lại máy server và đặt lại địa chỉ IP
Không hiển thị các dịch vụ TFTP và TPTP	Chưa cập nhật	Lưu và cập nhật
Không khởi động được	Do đặt sai biến khi cấu	Kiểm tra đặt lại và

router	hình router	quan sát quá trình khởi động
--------	-------------	------------------------------

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7. Đánh giá các bước thực hành

Bảng 5. 3: đánh giá các bước thực hành bài tập 5.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Khởi động phần mềm Cisco Packet Tracer	Chọn đúng biểu tượng			
2	Bước 2: Chọn thiết bị cấu hình như mô hình	Chuyển đúng thiết bị			
3	Bước 3: Kết nối Router và Server	Chọn đúng cổng kết nối			
4	Bước 4: Vào Router sau đó chuyển sang Tab CLI sau đó gõ lệnh Enable để chuyển sang chế độ đặt quyền	Bật chế chế độ mở			
5	Bước 5: Cấu hình địa chỉ IP và Subnet Mask cho Router	Nhập đúng địa chỉ IP và dòng lệnh			
6	Bước 6: Cấu hình cho Server	Chọn đúng tab			
7	Bước 7: Nhập địa chỉ IP và Subnet Mask	Chọn đúng chế độ và nhập IP			

	cho Server				
8	Bước 8:Ping Router qua server	Chuyển đúng chế độ, thực hiện ping và quan sát kết quả			
9	Bước 9:Ping Server qua Router	Chuyển đúng chế độ, thực hiện ping và quan sát kết quả			
10	Bước 10:Gõ lệnh write memory để lưu file cấu hình từ DRAM vào NVRAM	Nhập đúng dòng lệnh			
11	Bước 11:Bật dịch vụ TFTP trên máy chủ TFTP Server	Chọn đúng dịch vụ			
12	Bước 12:Copy IOS image mới vào bộ nhớ Flash của Router	Nhập đúng dòng lệnh và địa chỉ IP			
13	Bước 13:Đặt biến khởi động cho Router và ghi cấu hình	Chọn biến khởi động và quan sát quá trình khởi động			
14	Bước 14:Reload lại Router bằng cách sử dụng lệnh reload	Chọn đúng router			
15	Bước 15:Reload lại Router bằng cách sử dụng lệnh reload	Nhập đúng file hệ thống			

4.TÓM TẮT NỘI DUNG

- Xác định quá trình khởi động router.
- Nắm được các thiết bị Cisco tìm và tải IOS như thế nào.
- Sử dụng lệnh boot system.
- Xác định giá trị thanh ghi cấu hình.
- Xử lý sự cố.
- Xác định tập tin Cisco IOS và chức năng của nó.
- Nắm được các vị trí mà router lưu các loại tập tin khác nhau.

- Nắm được cấu trúc tên của IOS.
- Quản lý tập tin cấu hình bằng TFTP.
- Quản lý tập tin cấu hình bằng cắt – dán.
- Quản lý IOS bằng TFTP.
- Quản lý IOS bằng Xmodem.
- Kiểm tra tập tin hệ thống bằng các lệnh show.

5.CÂU HỎI VÀ BÀI TẬP

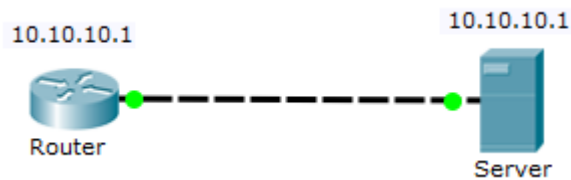
Câu hỏi:

Câu 1: Trình bày các giai đoạn khởi động router khi bắt đầu bật điện?

Câu 2: Nêu khái quát về tập tin hệ thống IOS?

Bài tập:

Cho mô hình mạng như hình :



- Thực hiện chép tập tin cấu hình khi sử dụng Hyper Terminal.
- Từ kết nối bằng HyperTerminal khôi phục lại tập tin cấu hình cho Router.
- Sử dụng Feature Cisco Navigator để kiểm tra Cisco IOS Feature

BÀI 6: ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN

Mã bài MD 28-06

Thời gian: 10 giờ

I. MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Giải thích được ý nghĩa của định tuyến tĩnh;
- Cấu hình đường cố định và đường mặc định cho router;
- Phân biệt các loại giao thức định tuyến;
- Xác định giao thức định tuyến theo vector khoảng cách;
- Cấu hình RIP cho router;
- Thực hiện các thao tác an toàn với máy tính;

II. NỘI DUNG GIẢNG DẠY

1. Giới thiệu về định tuyến tĩnh.

1.1 Giới thiệu về định tuyến tĩnh

- Định tuyến là quá trình mà router thực hiện để chuyển gói dữ liệu tới mạng đích. Tất cả các router dọc theo đường đi đều dựa vào địa chỉ IP đích của gói dữ liệu để chuyển gói theo đúng hướng đến đích cuối cùng. Để thực hiện được điều này, router phải học thông tin về đường đi tới các mạng khác. Nếu router chạy định tuyến động thì router tự động học những thông tin này từ các router khác. Còn nếu router chạy định tuyến tĩnh thì người quản trị mạng phải cấu hình các thông tin đến các mạng khác cho router.

- Đối với định tuyến tĩnh, các thông tin về đường đi phải do người quản trị mạng nhập cho router. Khi cấu trúc mạng có bất kỳ thay đổi nào thì chính người quản trị mạng phải xóa hoặc thêm các thông tin về đường đi cho router. Những loại đường đi như vậy gọi là đường đi cố định. Đối với hệ thống mạng lớn thì công việc bảo trì mạng định tuyến cho router như trên tốn rất nhiều thời gian. Còn đối với hệ thống mạng nhỏ, ít có thay đổi thì công việc này đỡ mất công hơn. Chính vì định tuyến tĩnh đòi hỏi người quản trị mạng phải cấu hình mọi thông tin về đường đi cho router nên nó không có được tính linh hoạt như định tuyến động. Trong những hệ thống mạng lớn, định tuyến tĩnh thường được sử dụng kết hợp với giao thức định tuyến động cho một số mục đích đặc biệt.

1.2 Hoạt động của định tuyến tĩnh

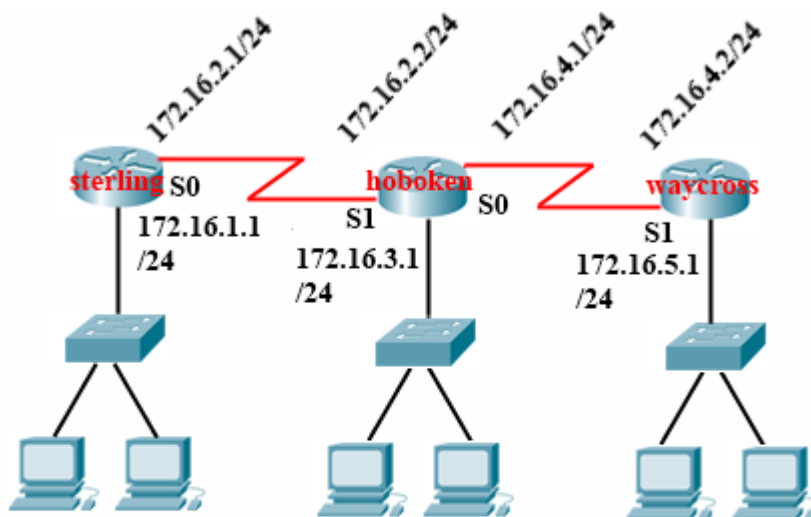
- Hoạt động của định tuyến tĩnh có thể chia ra làm 3 bước như sau:
 - + **Bước 1:** Đầu tiên, người quản trị mạng cấu hình các đường cố định cho router.
 - + **Bước 2:** Router cài đặt các đường đi này vào bảng định tuyến .
 - + **Bước 3:** Gói dữ liệu được định tuyến theo các đường cố định này .

- Người quản trị mạng cấu hình đường cố định cho router bằng lệnh ip route. Cú pháp của lệnh ip route như hình bên dưới.

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s0
command destination net subnet mask outgoing
interface
```

Hình 6. 1: Lệnh iproute

- Trong 2 hình 6.2. và 6.3 là 2 câu lệnh mà người quản trị của router Hoboken cấu hình đường cố định cho router đến mạng 172.16.1.0/24 và 172.16.5.0/24. Ở hình 6.2, câu lệnh này chỉ cho router biết đường đến mạng đích đi ra bằng cổng giao tiếp nào. Còn ở hình 6.3, câu lệnh này chỉ cho router biết địa chỉ IP của router kế tiếp là gì để đến được mạng đích. Cả 2 câu lệnh đều cài đặt đường cố định vào bảng định tuyến của router Hoboken. Điểm khác nhau duy nhất giữa 2 câu lệnh này là chỉ số tin cậy của 2 đường cố định tương ứng trên bảng định tuyến của router sẽ khác nhau.



```
Hoboken (config)#ip route 172.16.1.0 255.255.255.0 s1
command destination sub mask gateway
network

Hoboken (config)#ip route 172.16.5.0 255.255.255.0 s0
command destination sub mask gateway
network
```

Hình 6. 2: Cấu hình đường đi cố định

```
Hoboken (config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
command destination sub mask gateway
network

Hoboken (config)#ip route 172.16.5.0 255.255.255.0 172.16.4.2
command destination sub mask gateway
network
```

Hình 6. 3: Câu lệnh chỉ cho router biết địa chỉ IP của router kế tiếp

- Chỉ số tin cậy là một thông số đo lường độ tin cậy của một đường đi. Chỉ số này càng thấp thì độ tin cậy càng cao. Do đó, nếu đến cùng một đích

thì con đường nào có chỉ số tin cậy thấp hơn thì đường đó được vào bảng định tuyến của router trước. Trong ví dụ trên, đường cố định sử dụng địa chỉ IP của trạm kế tiếp sẽ có chỉ số tin cậy mặc định là 1, còn đường cố định sử dụng cổng ra thì có chỉ số tin cậy mặc định là 0. Nếu muốn chỉ định chỉ số tin cậy thay vì sử dụng giá trị mặc định thì thêm thông số này vào sau thông số về cổng ra/địa chỉ IP trạm kế của câu lệnh. Giá trị của chỉ số này nằm trong khoảng từ 0 đến 255.

```
Waycross (config)# ip route 172.16.3.0 255.255.255.0 172.16.4.1.130
```

- Nếu router không chuyển được gói ra cổng giao tiếp đã được cấu hình thì có nghĩa là cổng giao tiếp đang bị đóng, đường đi tương ứng cũng sẽ không được đặt vào bảng định tuyến.

- Đôi khi chúng ta sử dụng đường cố định làm đường dự phòng cho đường định tuyến động. Router sẽ chỉ sử dụng đường cố định khi đường định tuyến động bị đứt. Để thực hiện điều này, chỉ cần đặt giá trị chỉ số tin cậy của đường cố định cao hơn chỉ số tin cậy của giao thức định tuyến động đang sử dụng là được.

1.3 Cấu hình đường cố định

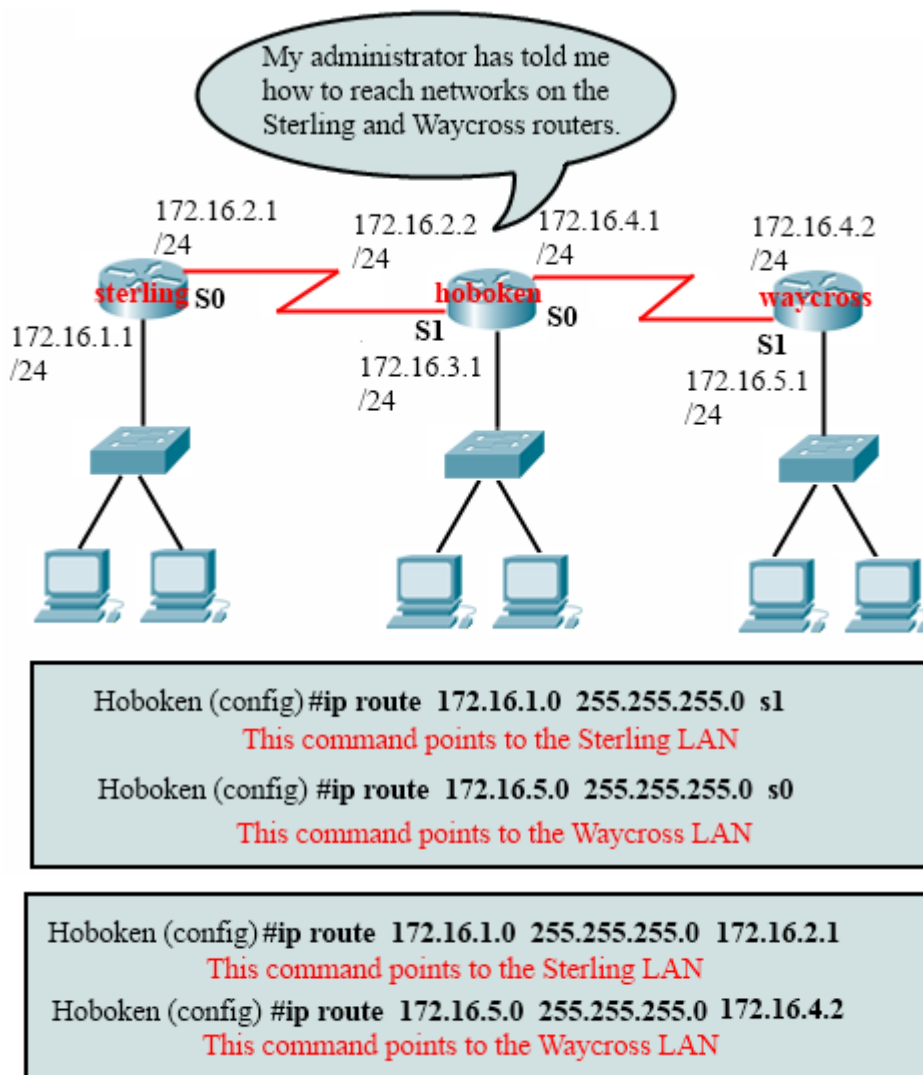
- Các bước để cấu hình đường cố định

- **Bước 1:** Xác định tất cả các mạng đích cần cấu hình, subnet mask tương ứng và gateway tương ứng. Gateway có thể là cổng giao tiếp trên router hoặc là địa chỉ của trạm kế tiếp để đến được mạng đích.
- **Bước 2:** vào chế độ cấu hình toàn cục của router.
- **Bước 3:** Nhập lệnh ip route với địa chỉ mạng đích, subnet mask tương ứng và gateway tương ứng mà đã xác định ở bước 1. Nếu cần thì thêm thông số về chỉ số tin cậy.
- **Bước 4:** Lặp lại bước 3 cho những mạng đích khác.
- **Bước 5:** Thoát khỏi chế độ cấu hình toàn cục.
- **Bước 6:** Lưu tập tin cấu hình đang hoạt động thành tập tin cấu hình khởi động bằng lệnh copy running –config statup-config.

- Hình 6.4 bên dưới là ví dụ về cấu hình đường cố định với cấu trúc mạng chỉ có 3 router kết nối đơn giản. Trên router Hoboken chúng ta phải cấu hình đường đi tới mạng.

172.16.1.0 và 172.16.5.0. Cả 2 mạng này đều có subnet mask là 255.255.255.0

- Khi router Hoboken định tuyến cho các gói đến mạng đích là 172.16.1.0 thì nó sử dụng các đường đi cố định mà ta đã cấu hình cho router để định tuyến tới router Sterling, còn gói nào đến mạng đích là 172.16.5.0 thì định tuyến tới router Waycross.



Hình 6. 4: Cấu hình đường đi cố định

- Ở khung phía trên của hình 6.4, cả 2 câu lệnh đều chỉ đường cố định cho router thông qua cổng ra trên router. Trong câu lệnh này lại không chỉ định giá trị cho chỉ số tin cậy nên trên bảng định tuyến 2 đường cố định nay có chỉ số tin cậy mặc định là 0. Đường có chỉ số tin cậy bằng 0 là tương đương với mạng kết nối trực tiếp vào router.

- Ở khung bên dưới của hình 6.4, 2 câu lệnh chỉ đường cố định cho router thông qua địa chỉ của router kế tiếp. Đường tới mạng 172.16.1.0 có địa chỉ của router kế tiếp là 172.16.2.1, đường tới mạng 172.16.5.0 có địa chỉ của router kế tiếp là: 172.16.4.2. Trong 2 câu này cũng không chỉ định giá trị cho chỉ số tin cậy nên 2 đường cố định tương ứng sẽ có chỉ số tin cậy mặc định là 1.

1.4 Cấu hình đường mặc định cho router chuyển gói đi

- Đường mặc định là đường mà router sẽ sử dụng trong trường hợp router không tìm thấy đường đi nào phù hợp trong bảng định tuyến để tới đích của gói dữ liệu chúng ta thường cấu hình đường mặc định cho đường ra Internet của router vì router không cần phải lưu thông tin định tuyến tới từng mạng trên Internet. Lệnh cấu hình đường mặc định thực chất cũng là lệnh cấu hình đường cố định, cụ thể là câu lệnh như sau:

Ip route 0.0.0.0.0.0.0[next –hop-address/outgoing interface]

- Subnet 0.0.0.0 khi được thực hiện phép toán AND logic với bất kỳ địa chỉ IP đích nào cũng có kết quả là mạng 0.0.0.0. Do đó, nếu gói dữ liệu có địa chỉ đích mà router không tìm được đường nào phù hợp thì gói dữ liệu đó sẽ được định tuyến tới mạng 0.0.0.0.

- Các bước cấu hình đường mặc định:

- **Bước 1:** Vào chế độ cấu hình toàn cục. Nhập lệnh ip route với mạng đích là 0.0.0.0 và subnet mask tương ứng là 0.0.0.0. Gateway của đường mặc định có thể là cổng giao tiếp trên router kế tiếp. Thông thường thì chúng ta nên sử dụng địa chỉ IP của router kế tiếp làm gateway.

- **Bước 2:** Thoát khỏi chế độ cấu hình toàn cục.

- **Bước 3:** Lưu lại thành tập tin cấu hình khởi động trong NVPAM bằng lệnh copy running –config.

- Tiếp tục xét ví dụ trong phần 6.4: router Hoboken đã được cấu hình để định tuyến dữ liệu tới mạng 172.16.1.0 trên router Sterling và tới mạng 1720160.5.0 trên router Waycross để chỉ đường tới từng mạng một. Nhưng cách này thì không phải là một giải pháp hay cho những hệ thống mạng lớn.

- Sterling kết nối đến tất cả các mạng khác thông qua một cổng Serial 0 mà thôi. Tương tự waycross cũng vậy. Waycross chỉ có một kết nối đến tất cả các mạng khác thông qua cổng Serial 1 mà thôi. Do đó chúng ta cấu hình đường mặc định cho Sterling và và Waycross thì 2 router này sẽ sử dụng đường mặc định để định tuyến cho gói dữ liệu đến tất cả các mạng nào không kết nối trực tiếp vào nó.

1.5 Kiểm tra cấu hình

- Sau khi cấu hình đường cố định, chúng ta phải kiểm tra xem bảng định tuyến đã có đường, cố định mà chúng ta đã cấu hình hay chưa, hoạt động định tuyến có đúng hay không. dùng lệnh show running –config để kiểm tra nội dung tập tin cấu hình đang chạy trên RAM xem câu lệnh cấu hình đường cố định đã được nhập vào đúng chưa. Sau đó dùng lệnh. Show ip route để xem có đường cố định trong bảng định tuyến hay không.

- Các bước kiểm tra cấu hình đường cố định:

- + **Bước 1:** Ở chế độ đặc quyền, nhập lệnh **show running-config** để xem tập tin cấu hình đang hoạt động.

- + **Bước 2:** Kiểm tra xem câu lệnh –cấu hình đường cố định có đúng không. Nếu không đúng thì phải vào lại chế độ cấu hình toàn cục, xóa câu lệnh sai đi và nhập lại câu lệnh mới.

- + **Bước 3:** Nhập lệnh **show ip route**.

- + **Bước 4:** Kiểm tra xem đường cố định mà đã cấu hình có trong bảng định tuyến hay không.

1.6 Xử lý sự cố

- Xét ví dụ trong phần 1.4: router Hoboken đã được cấu hình đường cố định tới mạng 172.16.1.0 trên Sterling và tới mạng 172.16.5.0 trên waycross. Với cấu hình như vậy thì node trong mạng 172.16.1.0 ở Sterling không thể truyền dữ liệu cho node trong mạng 172.16.5.0 được. Bây giờ trên router Sterling, thực hiện lệnh ping tới một node trong mạng 172.16.5.0. Lệnh ping không thành công. Sau đó dùng lệnh traceroute đến node mà vừa mới ping để xem lệnh traceroute bị rớt ở đâu. Kết quả của câu lệnh traceroute cho thấy router Sterling nhận được gói ICMP trả lời từ router Hoboken mà không nhận được từ router waycross. Chúng ta telnet vào router Hoboken. Từ router Hoboken chúng ta thử ping đến node trong mạng 172.16.5.0. Lệnh ping này sẽ thành công vì Hoboken kết nối trực tiếp với waycross.

2. Tổng quát về định tuyến

2.1 Giới thiệu về giao thức định tuyến

- Giao thức định tuyến khác với giao thức được định tuyến cả về chức năng và nhiệm vụ. Giao thức định tuyến được sử dụng để giao tiếp giữa các router với nhau.

- Giao thức định tuyến cho phép router này chia sẻ các thông tin định tuyến mà nó biết cho các router khác. Từ đó, các router có thể xây dựng và bảo trì bảng định tuyến của nó.

- Sau đây là một số giao thức định tuyến :

- Routing information Protocol(RIP)
- Interior Gateway Routing Protocol(IGRP)
- Enhanced Interior Gateway Routing Protocol(EIGRP)
- Open Shortest Path First(OSPF)

- Còn giao thức được định tuyến thì được sử dụng để định hướng cho dữ liệu của người dùng. Một giao thức được định tuyến sẽ cung cấp đầy đủ thông tin về địa chỉ lớp mạng để gói dữ liệu có thể truyền đi từ host này đến host khác dựa trên cấu trúc địa chỉ đó.

- Sau đây là các giao thức được định tuyến:

- Internet Protocol (IP)
- Internetwork Packet Exchange(IPX)

2.2 Autonomous system (AS) (Hệ thống tự quản)

- Hệ tự quản (AS) là một tập hợp các mạng hoạt động dưới cùng một cơ chế quản trị về định tuyến . Từ bên ngoài nhìn vào, một AS được xem như một đơn vị. Tổ chức Đăng ký số Internet của Mỹ (ARIN-American Registry of internet number là nơi quản lý việc cấp số cho mỗi AS. Chỉ này dài 16 Bit. Một số giao thức định tuyến, ví dụ như giao thức IRGP của Cisco, đòi hỏi phải có số AS xác định khi hoạt động.



Hình 6. 5: Một AS là bao gồm các router hoạt động dưới cùng một cơ chế quản trị

2.3 Mục đích của giao thức định tuyến và hệ thống tự quản

- Mục đích của giao thức định tuyến là xây dựng và bảo trì bảng định tuyến. Bảng định tuyến này mang thông tin về các mạng khác và các cổng giao tiếp trên router đến các mạng này. Router sử dụng giao thức định tuyến để quản lý thông tin nhận được từ các router khác, thông tin từ cấu hình của các cổng giao tiếp và thông tin cấu hình các đường cố định.

- Giao thức định tuyến cập nhật về tất cả các đường, chọn đường tốt nhất đặt vào bảng định tuyến và xoá đi khi đường đó không sử dụng được nữa. Còn router thì sử dụng thông tin trên bảng định tuyến để chuyển gói dữ liệu của các giao thức được định tuyến.

- Định tuyến động hoạt động trên cơ sở các thuật toán định tuyến. Khi cấu trúc mạng có bất kỳ thay đổi nào như mở rộng thêm, cấu hình lại, hay bị trục trặc thì khi đó ta nói hệ thống mạng đã được hội tụ. Thời gian để các router đồng bộ với nhau càng ngắn càng tốt vì khi các router chưa đồng bộ với nhau về các thông tin trên mạng thì sẽ định tuyến sai.

- Với hệ thống tự quản (AS), toàn bộ hệ thống mạng toàn cầu được chia ra thành nhiều mạng nhỏ, dễ quản lý hơn. Mỗi AS có một số AS riêng, không trùng lặp với bất kỳ AS khác, và mỗi AS có cơ chế quản trị riêng của mình.

2.4 Phân loại các giao thức định tuyến

- Đa số các thuật toán định tuyến được xếp vào 2 loại sau :

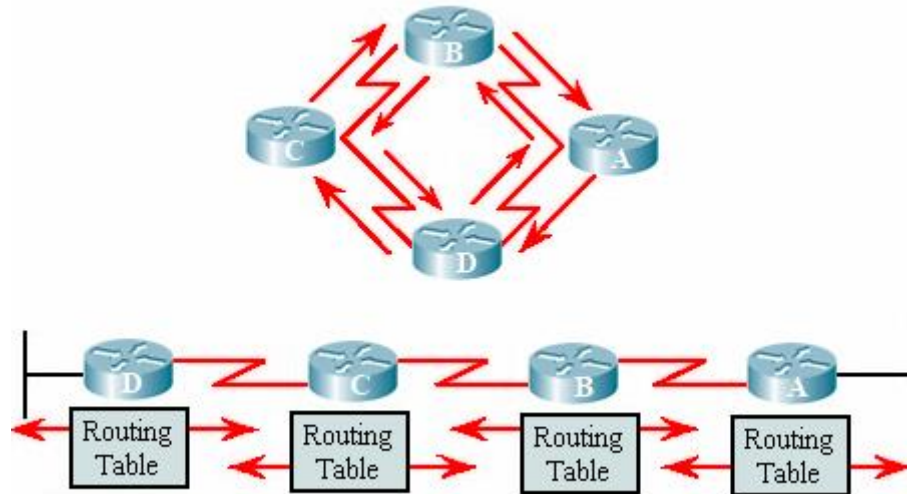
- + Vector khoảng cách.
- + Trạng thái đường liên kết.

- Định tuyến theo vector khoảng cách thực hiện truyền bản sao của bảng định tuyến từ router này sang router khác theo định kỳ. Việc cập nhật định kỳ giữa các router giúp trao đổi thông tin khi cấu trúc mạng thay đổi. Thuật toán định tuyến theo vector khoảng cách còn được gọi là thuật toán Bellman-Ford.

- Mỗi router nhận được bảng định tuyến của những router láng giềng kết nối trực tiếp với nó. Ví dụ như hình 6.6: router B nhận được thông tin từ router A. Sau đó router B sẽ cộng thêm khoảng cách từ router B đến router (ví

dụ như tăng số hop lên) vào các thông tin định tuyến nhận được từ A. Khi đó router B sẽ có bảng định tuyến mới và truyền bảng định tuyến này cho router láng giềng khác là router C. Quá trình này xảy ra tương tự cho tất cả các router láng giềng khác.

- Chuyển bảng định tuyến cho router láng giềng theo định kỳ và tính lại vector khoảng cách



Hình 6. 6: Router A nhận được thông tin về các mạng khác từ router B

- Router thu thập thông tin về khoảng cách đến các mạng khác, từ đó nó xây dựng và bảo trì một cơ sở dữ liệu về thông tin định tuyến trong mạng. Tuy nhiên, hoạt động theo thuật toán vector khoảng cách như vậy thì router sẽ không biết được chính xác cấu trúc của toàn bộ hệ thống mạng mà chỉ biết được các router láng giềng kết nối trực tiếp với nó mà thôi.

2.5 Đặc điểm của giao thức định tuyến theo vector khoảng cách

- Khi sử dụng định tuyến theo vector khoảng cách, bước đầu tiên là router phải xác định các router láng giềng với nó. Các mạng kết nối trực tiếp vào cổng giao tiếp của router sẽ có khoảng cách là 0. Còn đường đi tới các mạng không kết nối trực tiếp vào router thì router sẽ chọn đường tốt nhất dựa trên thông tin mà nó nhận được từ các router láng giềng. Ví dụ như hình vẽ 6.6: router A nhận được thông tin về các mạng khác từ router B. Các thông tin này được đặt trong bảng định tuyến với vector khoảng cách đã được tính toán lại cho biết từ router A đến mạng đích thì đi theo hướng nào, khoảng cách bao nhiêu.

- Bảng định tuyến được cập nhật khi cấu trúc mạng có sự thay đổi. Quá trình cập nhật này cũng diễn ra từng bước một từ router này đến router khác. Khi cập nhật, mỗi router gửi đi toàn bộ bảng định tuyến của nó cho các router láng giềng. Trong bảng định tuyến có thông tin về đường đi tới từng mạng đích: tổng chi phí cho đường đi, địa chỉ của router kế tiếp.

2.6 Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết

- Thuật toán định tuyến theo trạng thái đường liên kết là thuật toán Dijkstra hay còn gọi là thuật toán SPF (Shortest Path First tìm đường ngắn

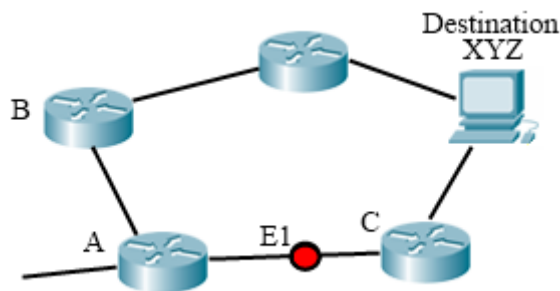
nhất). Thuật toán định tuyến theo trạng thái đường liên kết thực hiện việc xây dựng và bảo trì một cơ sở dữ liệu đầy đủ về cấu trúc của toàn bộ hệ thống mạng.

- Định tuyến theo trạng thái đường liên kết sử dụng những công cụ sau:
 - + Thông điệp thông báo trạng thái đường liên kết (LSA-Link-state Advertisement): LSA là một gói dữ liệu nhỏ mang thông tin định tuyến được truyền đi giữa các router .
 - + Cơ sở dữ liệu về cấu trúc mạng: được xây dựng từ thông tin thu thập được từ các LSA.
 - + Thuật toán SPF: dựa trên cơ sở dữ liệu về cấu trúc mạng, thuật toán SPF sẽ tính toán để tìm đường ngắn nhất.
 - + Bảng định tuyến: chứa danh sách các đường đi đã được chọn lựa.
- Quá trình thu thập thông tin mạng để thực hiện định tuyến theo trạng thái đường liên kết:
 - Mỗi router bắt đầu trao đổi LSA với tất cả các router khác, trong đó LSA mang cơ sở dữ liệu dựa trên thông tin của các LSA.
 - Mỗi router tiến hành xây dựng lại cấu trúc mạng theo dạng hình cây với bản thân nó là gốc, từ đó router vẽ ra tất cả các đường đi tới tất cả các mạng trong hệ thống. Sau đó thuật toán SPF chọn đường ngắn nhất để đưa vào bảng định tuyến. Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn với cổng ra tương ứng. Bên cạnh đó, router vẫn tiếp tục duy trì cơ sở dữ liệu về cấu trúc hệ thống mạng và trạng thái của các đường liên kết. Router nào phát hiện cấu trúc mạng thay đổi đầu tiên sẽ phát thông tin cập nhật cho tất cả các router khác. Router phát gói LSA, trong đó có thông tin về router mới, các thay đổi về trạng thái đường liên kết. Gói LSA này được phát đi cho tất cả các router khác.
 - Khi router nhận được gói LSA thì nó sẽ cập nhật lại cơ sở dữ liệu của nó với thông tin mới vừa nhận được. Sau đó SPF sẽ tính lại để chọn đường lại và cập nhật lại cho bảng định tuyến.
- Định tuyến theo trạng thái đường liên kết có một số nhược điểm sau:
 - + Bộ xử lý trung tâm của router phải tính toán nhiều
 - + Đòi hỏi dung lượng bộ nhớ phải lớn
 - + Chiếm dụng băng thông đường truyền
- Router sử dụng định tuyến theo trạng thái đường liên kết sẽ phải cần nhiều bộ nhớ hơn và hoạt động xử lý nhiều hơn là sử dụng định tuyến theo vector khoảng cách. Router phải có đủ bộ nhớ để lưu cơ sở dữ liệu về cấu trúc mạng, bảng định tuyến. Khi khởi động việc định tuyến, tất cả các router phải gửi gói LSA cho tất cả các router khác, khi đó băng thông đường truyền sẽ bị chiếm dụng làm cho băng thông dành cho đường truyền dữ liệu của người dùng bị giảm xuống. Nhưng sau khi các router đã thu thập đủ thông tin để xây

dụng cơ sở dữ liệu về cấu trúc mạng thì bảng thông đường truyền không bị chiếm dụng nữa. Chỉ khi nào cấu trúc mạng thay đổi thì router mới phát gói LSA để cập nhật và những gói LSA này chiếm một phần băng thông rộng rất nhỏ.

2.7 Quyết định chọn đường đi

- Router có 2 chức năng chính là:
 - + Quyết định chọn đường đi.
 - + Chuyển mạch.
- Quá trình chọn đường đi được thực hiện ở lớp Mạng. Router dựa vào bảng định tuyến để chọn đường cho gói dữ liệu, sau khi quyết định đường ra thì router thực hiện việc chuyển mạch để phát gói dữ liệu.
- Chuyển mạch là quá trình mà router thực hiện để chuyển gói từ cổng nhận vào ra cổng phát đi. Điểm quan trọng của quá trình này là router phải đóng gói dữ liệu cho phù hợp với đường truyền mà gói chuẩn bị đi ra.



Hình 6. 7: : router chọn đường cho gói dữ liệu

2.8 Cấu hình định tuyến

- Để cấu hình giao thức định tuyến, cần cấu hình trong chế độ cấu hình toàn cục và cài đặt các đặc điểm định tuyến. Bước đầu tiên, ở chế độ cấu hình toàn cục, cần khởi động giao thức định tuyến mà muốn, ví dụ: như RIP, IRGP, EIGRP hay OSPF. Sau đó, trong chế độ cấu hình định tuyến, công việc chính là khai báo địa chỉ IP. Định tuyến động thường sử dụng broadcast và multicast để trao đổi thông tin giữa các router. Router sẽ dựa vào thông số định tuyến để chọn đường tốt nhất tới từng mạng đích. Lệnh router dùng để khởi động giao thức định tuyến. Lệnh network dùng để khai báo các cổng giao tiếp trên router mà ta muốn giao thức định tuyến gửi và nhận các thông tin cập nhật về định tuyến. Sau đây là các ví dụ về cấu hình định tuyến:

```
GAD(config)#router rip
```

```
GAD(config-router)#network 172.16..0.0
```

- Địa chỉ mạng khai báo trong câu lệnh **network** là địa chỉ mạng theo lớp A, B hoặc C chứ không phải là địa chỉ mạng con(subnet) hay địa chỉ host riêng lẻ.

2.9 Các giao thức định tuyến

- Ở lớp Internet của bộ giao thức TCP/IP, router sử dụng một giao thức

định tuyến IP để thực hiện việc định tuyến. Sau đây là một số giao thức định tuyến **IP**:

- **RIP** - giao thức định tuyến nội theo vector khoảng cách.
 - **IGRP**- giao thức định tuyến nội theo vector khoảng cách Cisco.
 - **OSPF** - giao thức định tuyến nội theo trạng thái đường liên kết.
 - **EIGRP**- giao thức mở rộng của IGRP.
 - **BGP**- giao thức định tuyến ngoại theo vector khoảng cách.
- **RIP** (Routing information Protocol) được định nghĩa trong RFC 1058. Sau đây là các đặc điểm chính của RIP:
- Là giao thức định tuyến theo vector khoảng cách.
 - Sử dụng số lượng hop để làm thông số chọn đường đi.
 - Nếu số lượng hop để tới đích lớn hơn 15 thì gói dữ liệu sẽ bị huỷ bỏ.
 - Cập nhật theo định kỳ mặc định là 30 giây.
- **IGRP** (Internet gateway routing Protocol) là giao thức được phát triển độc quyền bởi Cisco. Sau đây là một số đặc điểm chính của IGRP:
- Là giao thức định tuyến theo vector khoảng cách.
 - Sử dụng băng thông, tải, độ trễ và độ tin cậy của đường truyền làm thông số lựa chọn đường đi.
 - Cập nhật theo định kỳ mặc định là 90 giây.
- **OSPF** (Open Shortest Path First) là giao thức định tuyến theo trạng thái đường liên kết. Sau đây là các đặc điểm chính của OSPF :
- Là giao thức định tuyến theo trạng thái đường liên kết.
 - Được định nghĩa trong RFC 2328.
 - Sử dụng thuật toán SPF để tính toán chọn đường đi tốt nhất .
 - Chỉ cập nhật khi cấu trúc mạng có sự thay đổi.
- **EIGRP** Là giao thức định tuyến nâng cao theo vector khoảng cách và là giao thức độc quyền của Cisco. Sau đây là các đặc điểm chính của EIGRP:
- Là giao thức định tuyến nâng cao theo vector khoảng cách, có chia tải.
 - Có các ưu điểm của định tuyến theo vector khoảng cách và định tuyến theo trạng thái đường liên kết.
 - Sử dụng thuật toán DUAL (Diffused Update Algorithm) để tính toán chọn đường tốt nhất. Cập nhật theo định kỳ mặc định là 90 giây hoặc cập nhật khi có thay đổi về cấu trúc mạng.
- **BGP** (Border Gateway Protocol) là giao thức định tuyến ngoại. Sau đây là các đặc điểm chính của BGP. Là giao thức định tuyến ngoại theo vector

khoảng cách.

- Được sử dụng để định tuyến giữa các ISP hoặc giữa ISP và khách hàng.
- Được sử dụng để định tuyến lưu lượng Internet giữa các hệ tự quản (AS).

2.10 Hệ tự quản, IGP và EGP

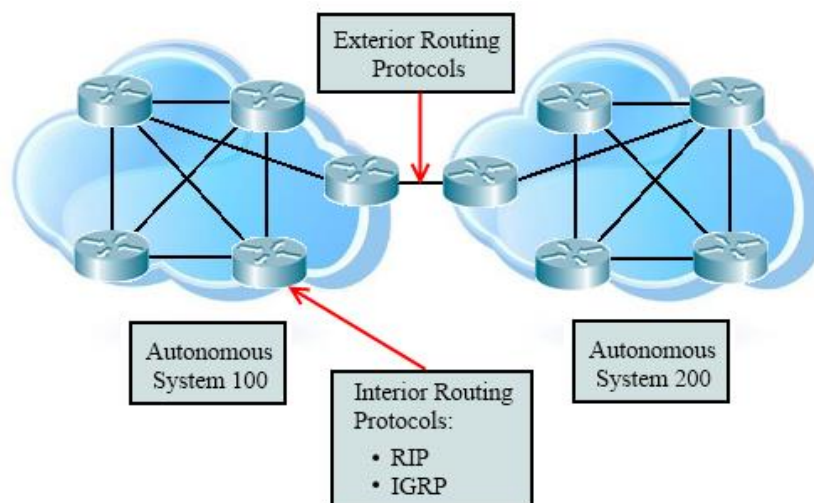
- Giao thức định tuyến nội được thiết kế để sử dụng cho hệ thống mạng của một đơn vị tổ chức mà thôi. Điều quan trọng nhất đối với việc xây dựng một giao thức định tuyến nội là chọn thông số nào và sử dụng những thông số đó ra sao để chọn đường đi trong hệ thống mạng.

- Giao thức định tuyến ngoại được thiết kế để sử dụng giữa 2 hệ thống mạng có 2 cơ chế quản lý khác nhau. Các giao thức loại này thường được sử dụng để định tuyến giữa các ISP. Giao thức định tuyến IP ngoại thường yêu cầu phải có 3 thông tin trước khi hoạt động, đó là:

- Danh sách các router láng giềng để trao đổi thông tin định tuyến.
- Danh sách các mạng kết nối trực tiếp mà giao thức cần quảng bá thông tin định tuyến.
- Chỉ số của hệ tự quản trên router.

- Giao thức định tuyến ngoại vì cần phải phân biệt các hệ tự quản. Các nên nhớ rằng mỗi hệ tự quản có một cơ chế quản trị riêng biệt. Giữa các hệ thống này phải có một giao thức để giao tiếp được với nhau.

- Mỗi một hệ tự quản có một con số xác định được cấp bởi tổ chức đăng ký số Internet của Mỹ (ARIN – America Registry of Internet Number) hoặc được cấp bởi nhà cung cấp dịch vụ. Con số này là số 16 bit. Các giao thức định tuyến như IGRP và EIGRP của Cisco đòi hỏi phải khai báo số AS khi cấu hình.



Hình 6. 8: hệ tự quản IRP và EGP

2.11 Trạng thái đường liên kết

- Thuật toán chọn đường theo trạng thái đường liên kết (hay còn gọi là

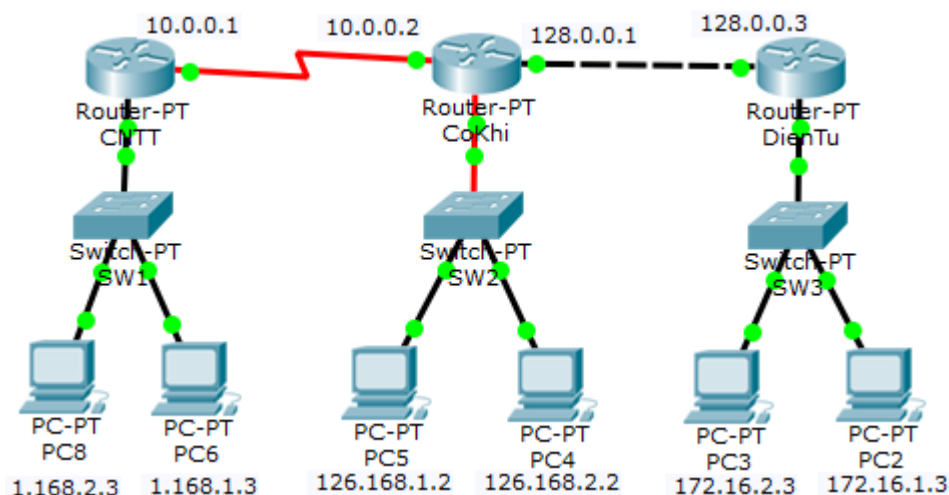
thuật toán chọn đường ngắn nhất) thực hiện trao đổi thông tin định tuyến cho tất cả các router khi bắt đầu chạy để xây dựng một bản đồ đầy đủ về cấu trúc hệ thống mạng. Mỗi router sẽ gửi gói thông tin tới tất cả các router còn lại. Các gói này mang thông tin về các mạng kết nối vào router. Mỗi router thu thập các thông tin này từ tất cả các router khác để xây dựng một bản đồ cấu trúc đầy đủ của hệ thống mạng. Từ đó router tự tính toán và chọn đường đi tốt nhất đến mạng đích để đưa lên bảng định tuyến. Sau khi toàn bộ các router đã được hội tụ thì giao thức định tuyến theo trạng thái đường liên kết chỉ sử dụng gói thông tin nhỏ để cập nhật, về sự thay đổi cấu trúc mạng chứ không gửi đi toàn bộ bảng định tuyến. Các gói thông tin cập nhật này được truyền đi cho tất cả các router khi có sự thay đổi xảy ra, do đó tốc độ hội tụ nhanh.

- Do tốc độ hội tụ nhanh hơn so với giao thức định tuyến theo vector khoảng cách, nên giao thức định tuyến theo trạng thái đường liên kết ít bị lặp vòng hơn. Mặc dù các giao thức loại này ít bị lỗi về định tuyến hơn nhưng lại tiêu tốn nhiều tài nguyên hệ thống hơn. Do đó chúng mắc tiền hơn nhưng bù lại chúng có khả năng mở rộng hơn so với giao thức định tuyến theo vector khoảng cách. Khi trạng thái của một đường liên kết nào đó thay đổi thì gói quảng bá trạng thái đường liên kết LSA được truyền đi trên khắp hệ thống mạng. Tất cả các router đều nhận được gói thông tin này và dựa vào đó để điều chỉnh lại việc định tuyến của mình. Phương pháp cập nhật như vậy tin cậy hơn, dễ kiểm tra hơn và tốn ít băng thông đường truyền hơn so với kiểu cập nhật của vector khoảng cách. OSPF và IS-IS là 2 giao thức định tuyến theo trạng thái đường liên kết.

3.BÀI TẬP THỰC HÀNH 6.1

3.1.Mô hình

- Cho mô hình mạng như hình 6.9:



Hình 6. 9: Mô hình PC kết nối Router

3.2.Yêu cầu

- + Cấu hình đường cố định cho các router bằng lệnh **ip route**.
- + Cấu hình giao thức định tuyến theo vector khoảng cách RIP.

3.3.Chuẩn bị:

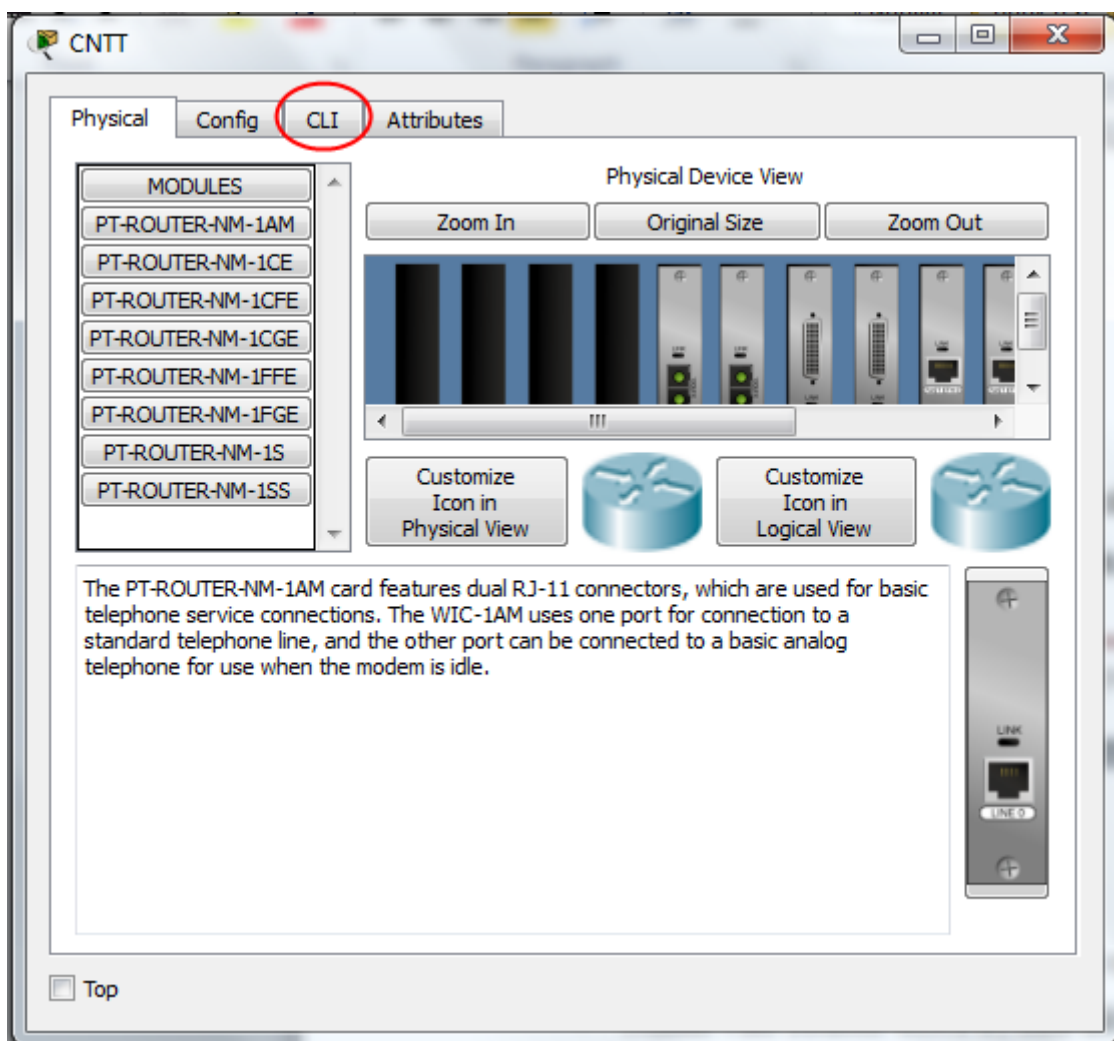
Bảng 6. 1: chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 6.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	6	
3	Router ảo	Cái	3	
4	Swicth ảo	Cái	3	

3.4.Các bước thực hành:

Bước 1: Cấu hình đường cố định cho router:

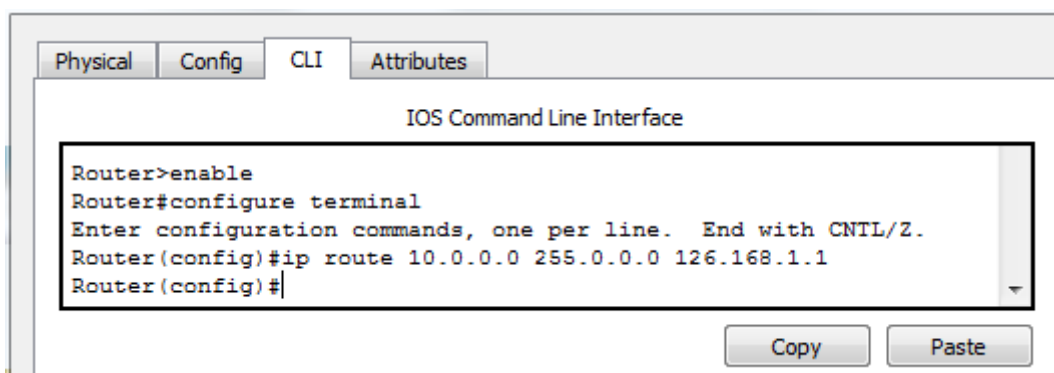
- Nhấn vào router CNTT, sau đó chuyển sang Tab CLI:



Hình 6. 10: Nhấn vào giao diện Router CNTT

Bước 2: Chuyển về chế độ toàn cục bằng cách gõ lệnh **configure terminal**

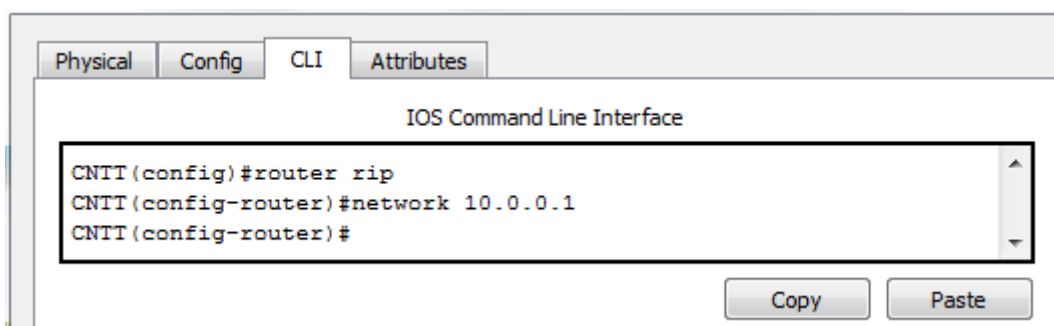
- Sau đó cài đặt đường đi vào bảng định tuyến,
- Từ bàn phím ta gõ lệnh **ip router [ip][subnet mask][next-hop-address/outgoing interface]** để cấu hình đường cố định cho router:



Hình 6. 11: Sử dụng lệnh ip route để cấu hình đường cố định

Bước 3: Cấu hình giao thức định tuyến vector khoảng cách:

- Từ chế độ cục bộ, ta gõ lệnh **router rip**
- Sau đó gõ tiếp lệnh **network <địa chỉ ip>**



Hình 6. 12: Cấu hình RIP

3.5.Những sự cố thường gặp

Bảng 6. 2: những sự cố thường gặp của bài tập 6.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không kết nối được PC với router	Chọn sai cổng kết nối	Chọn đúng cổng và bật chế độ mở
Không nhập được địa chỉ IP	Chọn sai máy server	Chọn lại máy server và đặt lại địa chỉ IP
Không cấu hình được chế độ toàn cục	Chưa cập nhật	Lưu và cập nhật
Không cấu hình được giao thức định tuyến	Đặt sai địa chỉ IP	Kiểm tra đặt lại địa chỉ IP và quan sát quá trình định tuyến

3.6.Báo cáo kết quả thực hành

.....

.....

.....

.....

3.7.Đánh giá các bước thực hành

Bảng 6. 3: đánh giá các bước thực hành bài tập 6.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1:Cấu hình đường cố định cho router	Chọn đúng port router			
2	Bước 2:Chuyển về chế độ toàn cục bằng cách gõ lệnh configure terminal	Gõ đúng lệnh			
3	Bước 3:Cấu hình giao thức định tuyến vectơ khoảng cách	Chọn đúng chế độ đặt quyền			

4.TÓM TẮT NỘI DUNG

- Router sẽ không chuyển gói tin nếu không tìm được đường tới đích.
- Đường cố định là do người quản trị mạng cấu hình cho router.
- Đường mặc định là một loại đặc biệt của đường cố định. Đường mặc định là con đường cuối cùng cho router sử dụng khi không tìm được đường nào tới đích.
- Ta có thể sử dụng các lệnh sau để kiểm tra cấu hình của đường cố định và đường mặc định: **show ip router, ping, traceroute**. Kiểm tra và xử lý sự cố.
- Các giao thức định tuyến.
- Giao thức định tuyến và hệ tự quản.
- Các loại giao thức định tuyến.
- Đặc điểm của giao thức định tuyến theo vectơ khoảng cách, trạng thái đường liên kết.
- Quyết định chọn đường đi.
- Cấu hình định tuyến.
- Các giao thức định tuyến: RIP, IGRP, OSPF, EIGRP, BGP.

- Định tuyến theo vectơ khoảng cách, đường liên kết.

5.CÂU HỎI VÀ BÀI TẬP

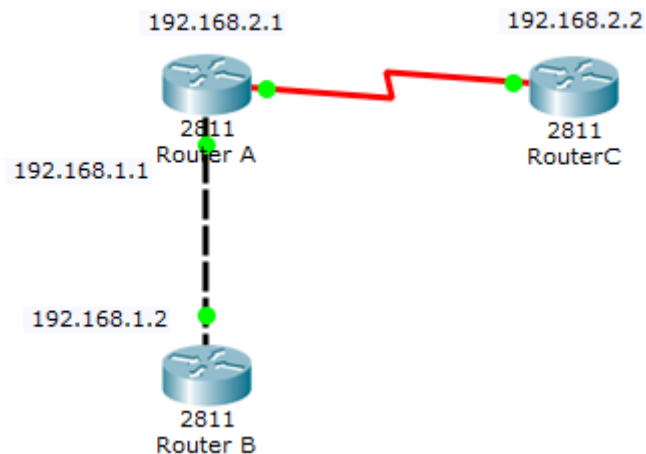
Câu hỏi:

Câu 1: Trình bày khái niệm định tuyến và hoạt động của định tuyến tĩnh?

Câu 2: Trình bày mục đích của giao thức định tuyến và hệ thống tự quản?

Bài tập:

Cho mô hình mạng như hình :



- Cấu hình Static Router.
- Cấu hình giao thức định tuyến EIGRP.
- Cấu hình OSPF cho Router Cisco

BÀI 7: GIAO THỨC ĐỊNH TUYẾN THEO VECTOR KHOẢNG CÁCH

Mã bài MD 28-07

Thời gian: 8 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

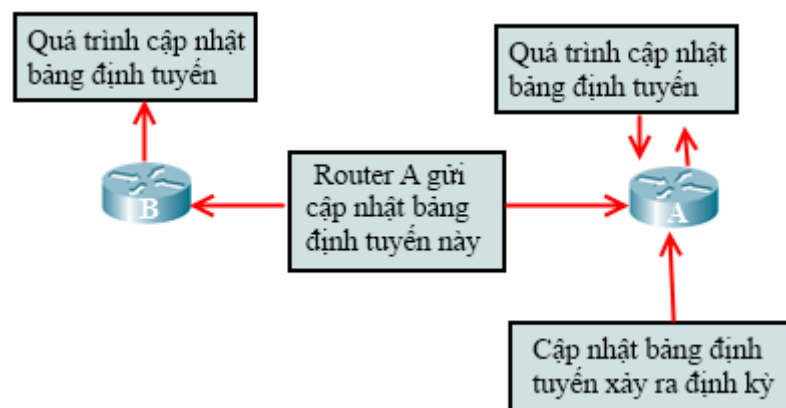
- Trình bày định tuyến vòng lặp;
- Xác định được các phương pháp được sử dụng để bảo đảm cho các giao thức định tuyến theo vector khoảng cách định tuyến đúng;
- Cấu hình RIP;
- Sử dụng lệnh IP classless;
- Cấu hình RIP để chia tải;
- Kiểm tra hoạt động của RIP;
- Thực hiện các thao tác an toàn với máy tính;

II.NỘI DUNG CHÍNH

1. Định tuyến theo vector khoảng cách.

1.1 Cập nhật thông tin định tuyến

- Bảng định tuyến được cập nhật theo chu kỳ hoặc khi cấu trúc mạng có sự thay đổi. Điểm quan trọng đối với một giao thức định tuyến là làm sao cập nhật bảng định tuyến một cách hiệu quả. Khi cấu trúc mạng thay đổi, thông tin cập nhật phải được xử lý trong toàn bộ hệ thống. Đối với định tuyến theo vector khoảng cách thì mỗi router gửi toàn bộ bảng định tuyến của mình cho các router kết nối trực tiếp với nó. Bảng định tuyến bao gồm các thông tin về đường đi tới mạng đích như: tổng chi phí(ví dụ như khoảng cách chẳng hạn) tính từ bản thân router đến mạng đích, địa chỉ của trạm kế tiếp trên đường đi.



Hình 7. 1: bảng định tuyến

1.2 Định nghĩa giá trị tối đa

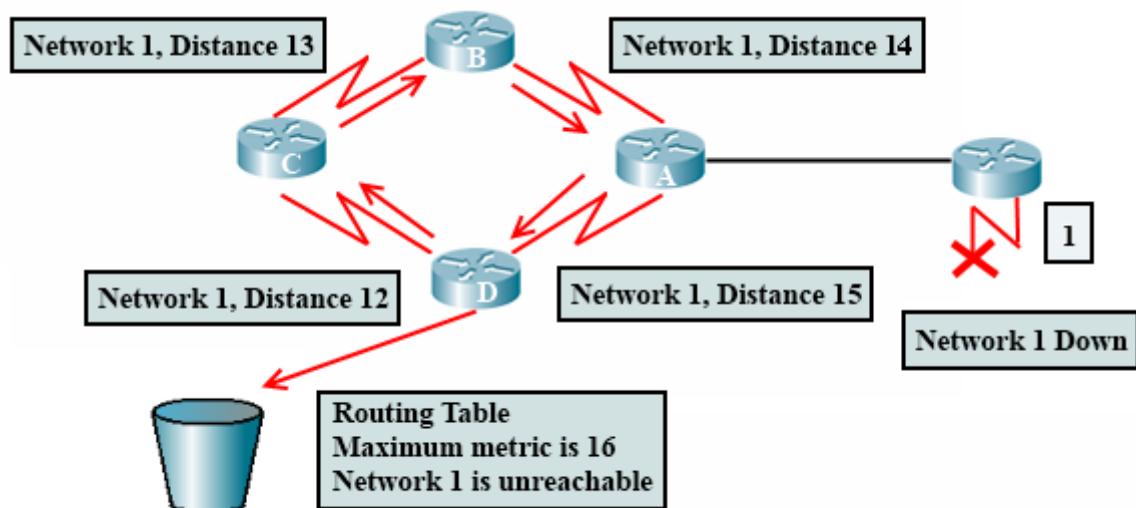
- Việc cập nhật sai về Mạng 1 như trên sẽ bị lặp vòng như vậy hoài cho đến khi nào có một tiến trình khác cắt đứt được quá trình này. Tình trạng như

vậy gọi là đếm vô hạn, gói dữ liệu sẽ bị lặp vòng trên mạng trong khi thực tế là mạng 1 đã bị ngắt.

- Với vector khoảng cách sử dụng thông số là số lượng hop thì mỗi khi router chuyển thông tin cập nhật cho router khác, chỉ số hop sẽ tăng lên 1. Nếu không có biện pháp khắc phục tình trạng đếm vô hạn, thì cứ như vậy chỉ số hop sẽ tăng lên đến vô hạn.

- Bản thân thuật toán định tuyến theo vector khoảng cách có thể tự sửa lỗi được nhưng quá trình lặp vòng này có thể kéo dài đến khi nào đếm đến vô hạn. Do đó để tránh tình trạng lỗi này kéo dài, giao thức định tuyến theo vector khoảng cách đã định nghĩa giá trị tối đa.

- Bằng cách này, giao thức định tuyến cho phép vòng lặp kéo dài đến khi thông số định tuyến vượt qua giá trị tối đa. Ví dụ như hình vẽ dưới, khi thông số định tuyến là 16 hop lớn hơn giá trị tối đa là 15 thì thông tin cập nhật đó sẽ bị router huỷ bỏ. Trong bất kỳ trường hợp nào, khi giá trị của thông số định tuyến vượt qua giá trị tối đa thì xem như mạng đó là không đến được.



Chỉ định số liệu vector khoảng cách tối đa là vô cực

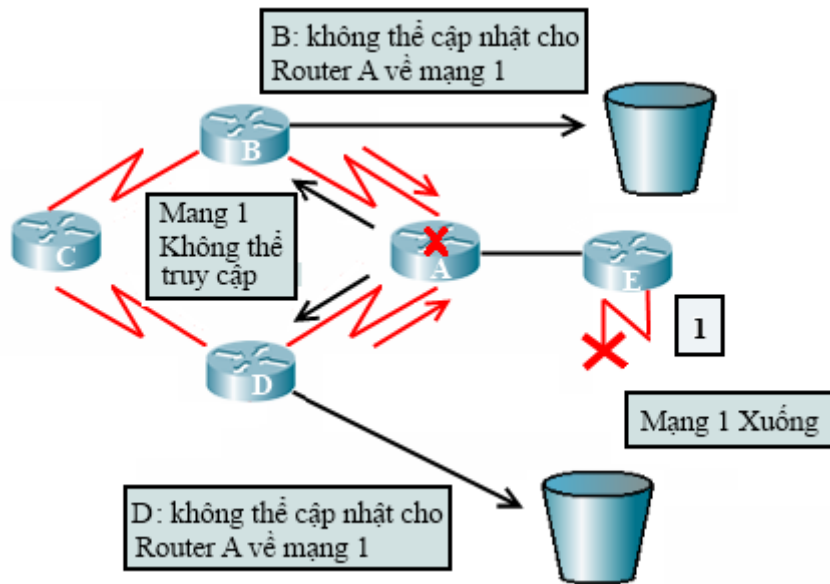
Hình 7. 2: Thông số định tuyến

1.3 Tránh định tuyến lặp vòng bằng split horizon

- Một nguyên nhân khác gây ra lặp vòng là router gửi lại những thông tin định tuyến mà nó vừa nhận được cho chính router đã gửi những thông tin đó. Phần sau đây sẽ phân tích cho các thấy sự cố xảy ra như thế nào.

1. Router A gửi một thông tin cập nhật cho router B và D thông báo là Mạng 1 đã bị ngắt. Tuy nhiên router C vẫn gửi cập nhật cho router B là router C có đường đến Mạng 1 thông tin qua router D, khoảng cách của đường này là 4.
2. Khi đó router B tưởng lầm là router C vẫn có đường đến Mạng 1 mặc dù con đường này có thông số định tuyến không tốt bằng con đường cũ của router B lúc trước. Sau đó router B cũng cập nhật cho router A về đường mới đến Mạng 1 mà router B vừa mới nhận được.

3. Khi đó router A sẽ cập nhật lại là nó có thể gửi dữ liệu đến Mạng 1 thông qua router B. Router B thì định tuyến đến Mạng 1 thông qua router C. Router C lại định tuyến đến Mạng 1 thông qua router D. Kết quả là bất kỳ gói dữ liệu nào đến Mạng 1 sẽ rơi vào vòng lặp này.
4. Cơ chế split-horizon sẽ tránh được tình huống này bằng cách: Nếu router B hoặc D nhận được thông tin cập nhật về Mạng 1 từ router A thì chúng sẽ không gửi lại thông tin cập nhật về Mạng 1 cho router A nữa. Nhờ đó, split-horizon làm giảm được việc cập nhật thông tin sai và giảm bớt việc xử lý thông tin cập nhật.



Hình 7. 3: Cơ chế split-horizon

1.4 Router poisoning

- Route poisoning được sử dụng để tránh xảy ra các vòng lặp lớn và giúp cho router thông báo thẳng là mạng đã không truy cập được nữa bằng cách đặt giá trị cho thông số định tuyến (số lượng hop chẳng hạn) lớn hơn giá trị tối đa.

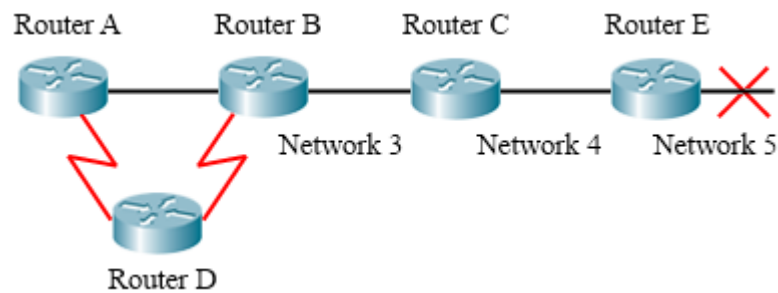
- Ví dụ như hình 7.4: Khi Mạng 5 bị ngắt thì trên bảng định tuyến của router E giá trị hop cho đường đến Mạng 5 là 16, giá trị này có nghĩa là Mạng 5 không truy cập được nữa. Sau đó router E cập nhật cho router C bảng định tuyến này, trong đó đường đến Mạng 5 có thông số hop là 16 được gọi là route poisoning. Sau khi router C nhận được cập nhật về route poisoning từ router E, router C sẽ gửi ngược trở lại thông tin này cho router E. Lúc này ta gọi thông tin cập nhật về Mạng 5 từ router C gửi ngược lại cho router E là route poison reverse. Router C làm như vậy để đảm bảo là nó đã gửi thông tin route poisoning ra tất cả các đường mà nó có.

- Khi route poisoning được sử dụng kết hợp với cập nhật tức thời sẽ giúp rút ngắn thời gian hội tụ giữa các router vì khi đó router không cần phải chờ hết 30 giây của chu kỳ cập nhật mới về route poisoning.

- Tóm lại: Route poisoning có nghĩa là khi có một con đường nào đó bị ngắt thì router sẽ thông báo về con đường đó với thông số định tuyến lớn hơn

giá trị tối đa. Cơ chế route poisoning không hề gây mâu thuẫn với cơ chế split horizon. Split horizon có nghĩa là khi router gửi thông tin cập nhật ra một đường liên kết thì router không được gửi lại những thông tin nào mà nó vừa nhận vào từ đường liên kết đó. Bây giờ, router vẫn gửi lại những thông tin đó nhưng với thông số định tuyến lớn hơn giá trị tối đa thì kết quả vẫn như vậy. Cơ chế này gọi là split horizon kết hợp với poison reverse.

- Khi mạng 5 bị ngắt, Router E sử dụng route poisoning bằng cách đặt giá trị 16 trên bảng định tuyến để cho biết mạng này không đến được nữa.



Hình 7. 4: Thông tin route poisoning

1.5 Tránh định tuyến lặp vòng bằng cơ chế cập nhật tức thời

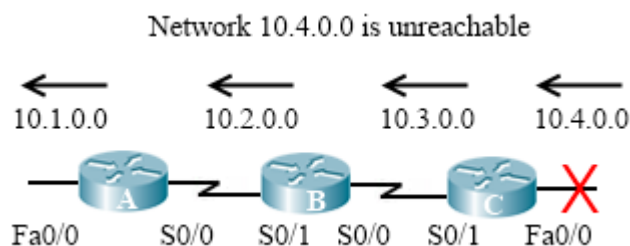
- Hoạt động cập nhật bảng định tuyến giữa các router láng giềng được thực hiện theo chu kỳ. Ví dụ: cứ sau 30 giây RIP thực hiện cập nhật một lần. Ngoài ra còn có cơ chế cập nhật tức thời để thông báo về một thay đổi nào đó trong bảng định tuyến. Khi router phát hiện ra có một thay đổi nào đó trong cấu trúc thì nó lập tức gửi thông điệp cập nhật cho các router láng giềng để thông báo về sự thay đổi đó. Nhất là khi có một đường nào đó bị lỗi không truy cập được nữa thì router phải cập nhật tức thời thay vì đợi đến hết chu kỳ. Cơ chế cập nhật tức thời kết hợp với route poisoning sẽ đảm bảo cho tất cả các router nhận được thông tin khi có một đường nào đó bị ngắt trước khi thời gian holddown kết thúc.

- Cơ chế cập nhật tức thời cho toàn bộ mạng khi có sự thay đổi trong cấu trúc mạng giúp cho các router được cập nhật kịp thời và khởi động thời gian holddown nhanh hơn.

- Ví dụ như hình 7.5: router C cập nhật tức thời ngay khi mạng 10.4.0.0 không truy cập được nữa. Khi nhận được thông tin này, router B cũng phát thông báo về mạng 10.4.0.0 ra cổng S0/1. Đến lượt router A cũng sẽ phát thông báo ra cổng Fa0/0.

NetWordk 10.4.0.0 is unreachable

- Với cập nhật tức thời, router sẽ gửi thông điệp ngay để thông báo sự thay đổi trong bảng định tuyến của mình.



Hình 7. 5: Cơ chế cập nhật tức thời

1.6 Tránh lặp vòng với Thời gian holddown

- Khi router nhận được từ router láng giềng một thông tin cho biết là một mạng X nào đó bây giờ không truy cập được nữa thì router sẽ đánh dấu vào con đường tới mạng X đó là không truy cập được nữa và khởi động thời gian holddown. Trong khoảng thời gian holddown này, nếu router nhận được thông tin cập nhật từ chính router láng giềng lúc này thông báo là mạng X đã truy cập lại được thì router mới cập nhật thông tin đó và kết thúc thời gian holddown.

- Trong suốt thời gian holddown nếu router nhận được thông tin cập nhật từ một router láng giềng khác (không phải là router láng giềng đã phát thông tin cập nhật về mạng X lúc này) nhưng thông tin này cho biết có đường đến mạng X với thông số định tuyến tốt hơn con đường mà router trước đó thì nó sẽ bỏ qua, không cập nhật thông tin này. Cơ chế này giúp cho router tránh được việc cập nhật nhầm những thông tin cũ do các router láng giềng chưa hay biết gì về việc mạng X đã không truy cập được nữa. Không thời gian holddown bảo đảm cho tất cả các router trong hệ thống mạng đã được cập nhật xong về thông tin mới. Sau khi thời gian holddown hết thời hạn, tất cả các router trong hệ thống đều đã được cập nhật là mạng X không truy cập được nữa, khi đó các router đều có thể nhận biết chính xác về cấu trúc mạng. Do đó, sau khi thời gian holddown kết thúc thì các router lại cập nhật thông tin như bình thường.

2. RIP

2.1 Tiến trình của RIP

- IP RIP được mô tả chi tiết trong 2 văn bản. Văn bản đầu tiên là RFC1058 và văn bản thứ 2 là Tiêu chuẩn Internet(STD)56.

- RIP được phát triển trong nhiều năm bắt đầu từ phiên bản 1 (RIPv1).
- RIP chỉ là giao thức định tuyến theo lớp địa chỉ cho đến phiên bản 2(RIPv2).

- RIP trở thành giao thức định tuyến không theo lớp địa chỉ. RIPv2 có những ưu điểm hơn như sau:

- Cung cấp thêm nhiều thông tin định tuyến hơn.
- Có cơ chế xác minh giữa các router khi cập nhật để bảo mật cho bảng định tuyến.
- Có hỗ trợ VLSM(variable Length Subnet Masking-Subnet mask có chiều dài khác nhau).

- RIP tránh định tuyến lặp vòng đếm đến vô hạn bằng cách giới hạn số lượng hop tối đa cho phép từ máy gửi đến máy nhận, số lượng hop tối đa cho mỗi con đường là 15. Đối với các con đường mà router nhận được từ thông tin cập nhật của router láng giềng, router sẽ tăng chỉ số hop lên 1 vì router xem bản thân nó cũng là 1 hop trên đường đi. Nếu sau khi tăng chỉ số hop lên 1 mà chỉ số này lớn hơn 15 thì router sẽ xem như mạng đích không tương ứng với con đường này không đến được. Ngoài ra, RIP cũng có những đặc tính tương tự như các giao thức định tuyến khác. Ví dụ như: RIP cũng có horizon và thời gian holddown để tránh cập nhật thông tin định tuyến không chính xác.

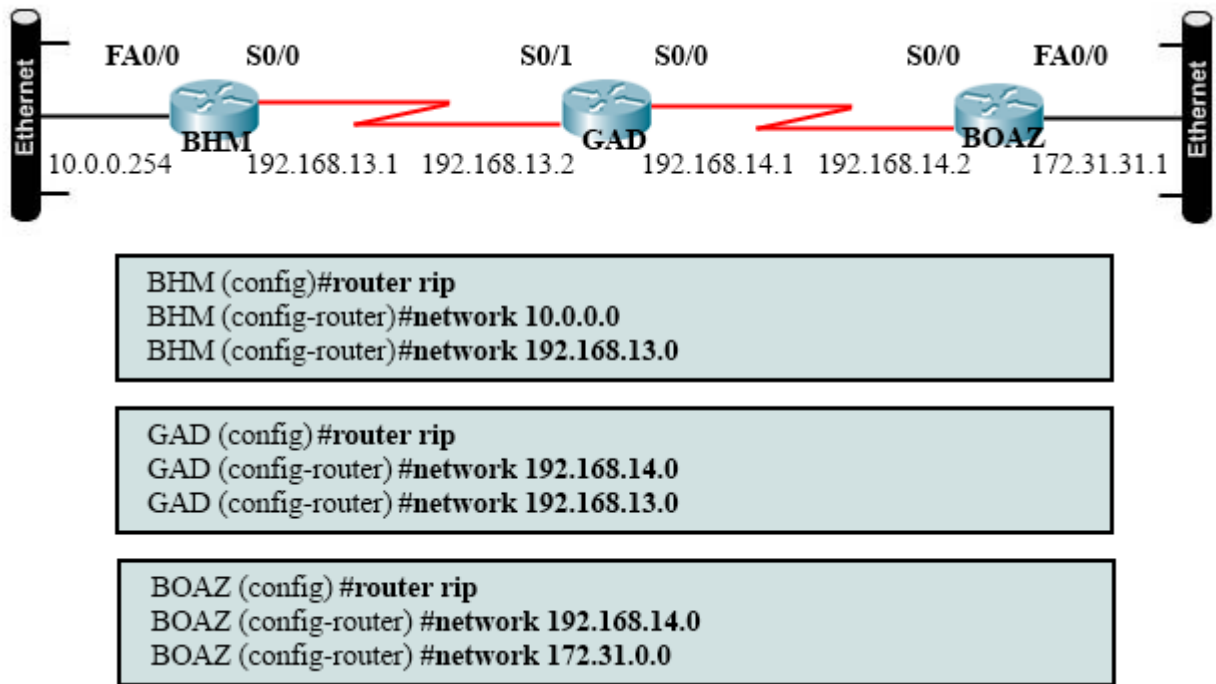
Các đặc điểm chính của RIP
• Là giao thức định tuyến theo vectơ khoảng cách. • Thông số định tuyến là số lượng hop. • Nếu gói dữ liệu đến mạng đích có số lượng hop lớn hơn 15 thì gói dữ liệu đó sẽ bị huỷ bỏ. • Chu kỳ cập nhật mặc định là 30 giây.

2.2 Cấu hình RIP

- **Lệnh** router rip dùng để khởi động RIP. Lệnh network dùng để khai báo những cổng giao tiếp nào của router được phép chạy RIP trên đó. Từ đó RIP sẽ bắt đầu gửi và nhận thông tin cập nhật trên các cổng tương ứng RIP cập nhật thông tin định tuyến theo chu kỳ. Khi router nhận được thông tin cập nhật có sự thay đổi nào đó thì nó sẽ cập nhật thông tin mới vào bảng định tuyến. Đối với những con đường tới mạng đích mà router học được từ router láng giềng thì nó sẽ tăng chỉ số hop lên 1 địa chỉ nguồn của thông tin cập nhật này sẽ là địa chỉ trạm kế tiếp RIP, chỉ chọn một con đường tốt nhất đến mạng đích, tuy nhiên nó cũng có thể sử dụng nhiều con đường có chỉ số bằng nhau đến cùng 1 đích.

- Chúng ta có thể cấu hình cho RIP thực hiện cập nhật tức thời khi cấu trúc mạng thay đổi bằng lệnh ip rip triggered, lệnh này chỉ áp dụng cho cổng serial của router. Khi cấu trúc mạng thay đổi, router nào nhận biết được sự thay đổi đầu tiên sẽ cập nhật vào bảng định tuyến của nó trước, sau đó nó lập tức gửi thông tin cập nhật cho các router khác để thông báo về sự thay đổi đó. Hoạt động này là cập nhật tức thời và nó xảy ra hoàn toàn độc lập với cập nhật định kỳ.

- Hình 7.6 là một ví dụ về cấu hình của RIP.



Hình 7. 6: Cấu hình RIP

- BHM(config)#router rip- chọn RIP làm giao thức định tuyến cho router.
 - BHM(config- router)#network10.0.0.0- khai báo mạng kết nối trực tuyến vào router.
 - BHM (config- router) #network 192.168.13.0-khai báo mạng kết nối trực tuyến vào router.
- Các cổng trên router kết nối vào mạng 10.0.0.0 và 192.168.13.0 sẽ thực hiện gửi và nhận thông tin cập nhật về định tuyến.
- Sau khi đã khởi động RIP trên các mạng rồi chúng ta có thể thực hiện thêm một số cấu hình khác. Những cấu hình này không bắt buộc phải làm, chúng ta chỉ cấu hình thêm nếu thấy cần thiết:
- Điều chỉnh các thông số định tuyến.
 - Điều chỉnh các thông số về thời gian hoạt động của RIP.
 - Khai báo phiên bản của RIP mà ta đang sử dụng(RIPv1 hay RIPv2).
 - Cấu hình cho RIP chỉ gửi thông tin định tuyến rút gọn cho một cổng nào đó.
 - Kiểm tra thông tin định tuyến IP rút gọn.
 - Cấu hình cho IGRP và RIP chạy đồng thời .
 - Không cho phép RIP nhận thông tin cập nhật từ một địa chỉ IP nào đó.
 - Mở hoặc tắt chế độ split horizon.
 - Kết nối RIP vào mạng WAN.

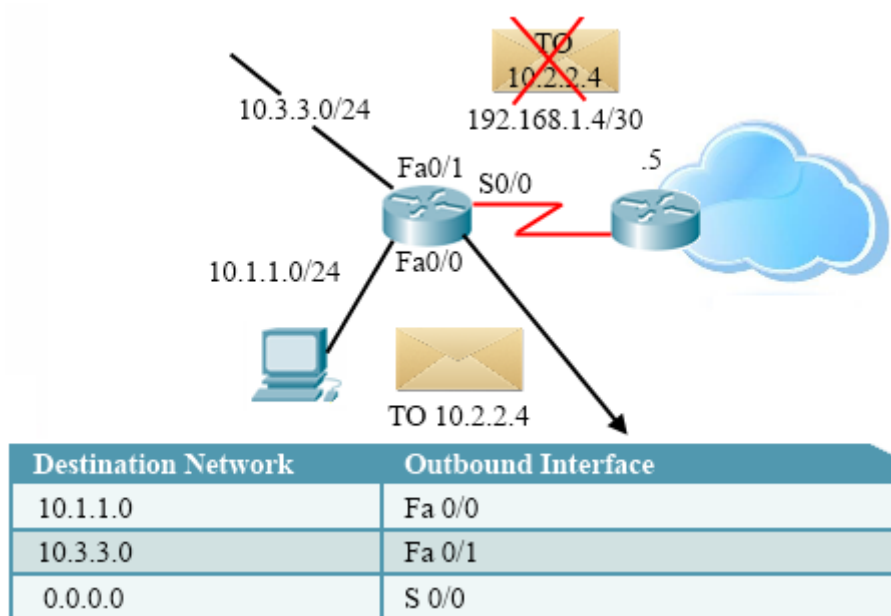
- Tóm lại, để cấu hình RIP, chúng ta có thể bắt đầu từ chế độ cấu hình toàn cục như sau:

- Router(config)# router rip – khởi động giao thức định tuyến RIP.
- Router(config-router)#network network-number- khai báo các mạng mà RIP được phép chạy trên đó.

2.3 Sử dụng lệnh ip classless

- Khi router nhận được gói dữ liệu có địa chỉ đích là một subnet không có trên bảng định tuyến của router. Trên bảng định tuyến của router không có chính xác subnet với subnet đích của gói dữ liệu. Ví dụ: một tổ chức sử dụng địa chỉ mạng 10.10.0.0/16, khi đó subnet 10.10.10.0/24 có supernet là 10.10.0.0/16. Trong trường hợp như vậy, ta dùng lệnh ip classless để router không hủy bỏ dữ liệu mà sẽ chuyển gói ra đường đến địa chỉ supernet, nếu có. Đối với phần mềm Cisco IOS phiên bản 11.3 trở về sau, mặc định là lệnh ip classless đã được chạy trong cấu hình của router. Nếu tắt lệnh này đi thì dùng lệnh NO của câu lệnh này.

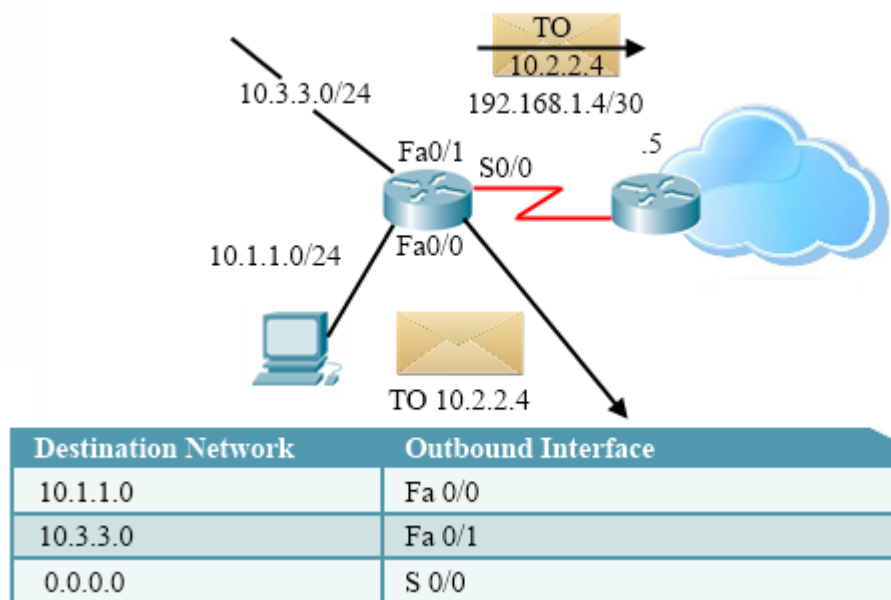
- Tuy nhiên, nếu không có chức năng này thì tất cả các gói có địa chỉ đích là một subnet có cùng supernet với các địa chỉ mạng khác của router nhưng lại không có trong bảng định tuyến. Đây chính là đặc điểm quan trọng của giao thức định tuyến theo lớp. Nếu một địa chỉ mạng lớn được chia thành các subnet con chứ không có toàn bộ các subnet. Khi đó gói dữ liệu nào có địa chỉ đích là một subnet nằm trong địa chỉ mạng lớn nhưng lại không có trên bảng định tuyến của router thì router sẽ hủy bỏ.



Hình 7. 7: khi không có lệnh ip classless

- Cơ chế này bị nhầm lẫn nhất khi router có cấu hình đường mặc định. Từ một địa chỉ mạng lớn chia thành nhiều subnet con. Kết nối trực tiếp vào router chỉ có một số subnet. Khi router xây dựng bảng định tuyến, trên bảng định tuyến đương nhiên có các subnet của mạng kết nối trực tiếp vào router. Còn những subnet nào không có thì router coi như subnet đó không tồn tại.

Do đó, khi router nhận được gói dữ liệu có địa chỉ đích là một subnet không có trên bảng định tuyến nhưng lại có cùng supernet với các mạng kết nối trực tiếp vào router thì router xem như mạng đích đó không tồn tại và hủy bỏ gói dữ liệu cho dù trên bảng định tuyến của router có cấu hình đường mặc định. Lệnh ip classless sẽ giải quyết vấn đề này bằng cách cho phép router không cần quan tâm đến lớp của địa chỉ đích nữa. Khi đó router không tìm thấy được cụ thể mạng đích trên bảng định tuyến thì nó sẽ sử dụng đường mặc định để chuyển gói đi.



Hình 7. 8: khi có lệnh ip classless

2.4 Những vấn đề thường gặp khi cấu hình RIP

- Router định tuyến theo RIP phải dựa vào các router láng giềng để học thông tin đến các mạng mà không kết nối trực tiếp vào router. RIP sử dụng thuật toán định tuyến theo vector khoảng cách để có nhược điểm chính tốc độ hội tụ chậm. Trạng thái hội tụ là khi tất cả các router trong hệ thống mạng đều có thông tin định tuyến về hệ thống mạng giống nhau và chính xác.
- Các giao thức định tuyến theo vector khoảng cách thường gặp vấn đề về định tuyến lặp vòng và đếm đến vô hạn. Đây là hậu quả khi các router chưa được hội tụ nên truyền cho nhau những thông tin cũ chưa được cập nhật đúng.
- Để giải những vấn đề này RIP sử dụng những kỹ thuật sau:
 - + Định nghĩa giá trị tối đa.
 - + Split horizon.
 - + Poison reverse.
 - + Thời gian holddown.
 - + Cập nhật tức thời.
- Có một số kỹ thuật đòi hỏi phải cấu hình còn một số khác thì không cần cấu hình gì cả hoặc chỉ cần cấu hình một chút thôi.

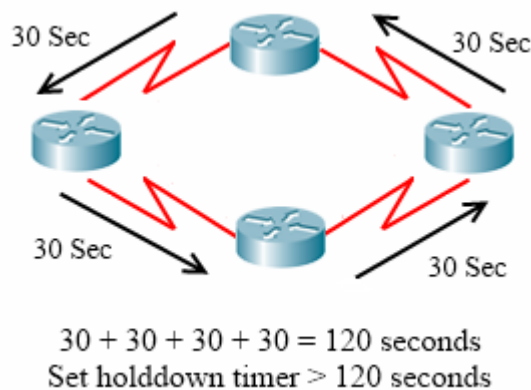
- RIP giới hạn số hop tối đa là 15. Bất kỳ mạng đích nào có số hop lớn hơn 15 thì xem như mạng đó không đếm được. Điều này làm cho RIP bị hạn chế không sử dụng được cho những hệ thống mạng lớn nhưng nó giúp cho RIP tránh được lỗi đếm đến vô hạn.

- Luật split horizon là: khi gửi thông tin cập nhật ra một hướng nào đó thì không gửi lại những thông tin mà router đã nhận được từ hướng đó. Trong một số cấu hình mạng thì cần phải tắt cơ chế split horizon: `GAD (config-if)#no ip split-horizon`.

- Thời gian holddown là một thông số mà có thể thay đổi nếu cần. Khoảng thời gian holddown giúp cho router tránh bị lặp vòng đếm đến vô hạn nhưng đồng thời nó cũng làm tăng thời gian hội tụ giữa các router. Trong khoảng thời gian này, router không cập nhật những đường nào có thông số định tuyến không tốt bằng con đường mà router có trước đó, như vậy thì có khi có đường khác thay thế cho đường cũ thật nhưng router cũng không cập nhật. Thời gian holddown mặc định của RIP là 180 giây. có thể điều chỉnh thời gian holddown ngắn lại để tăng tốc độ hội tụ nhưng nên cân nhắc kỹ. Thời gian holddown lý tưởng là phải dài hơn khoảng thời gian dài nhất có thể để cho toàn bộ hệ thống mạng được cập nhật xong. Ví dụ như hình dưới, chúng ta có 4 router. Nếu mỗi router có thời gian cập nhật là 30 giây thì thời gian tối đa để cho cả 4 router cập nhật xong là 120 giây như vậy thời gian holddown phải dài hơn 120 giây.

- Để thay đổi thời gian holddown dùng lệnh sau:

`Router(config-router)#timers basic update invalid holddown flush[sleeptime]`



Hình 7. 9: Thời gian cập nhật router

- Một lý do khác làm ảnh hưởng đến tốc độ hội tụ là chu kỳ cập nhật. Chu kỳ cập nhật mặc định của RIP là 30 giây. Có thể điều chỉnh cho chu kỳ cập nhật dài hơn để tiếp kiệm băng thông đường truyền hoặc rút ngắn chu kỳ cập nhật lại để tăng tốc độ hội tụ.

- Để thay đổi chu kỳ cập nhật, dùng lệnh sau:

`GAD(config-router)#update-timer seconds`

- Còn một vấn đề nữa mà ta thường gặp đối với giao thức định tuyến là ta không muốn cho các giao thức này gửi các thông tin cập nhật về định tuyến ra

một cổng nào đó. Sau khi nhập lệnh network để khai báo địa chỉ mạng là lập tức RIP bắt đầu gửi các thông tin định tuyến ra tất cả các cổng có địa chỉ mạng nằm trong mạng mà vừa khai báo. Nhà quản trị mạng có thể không cho phép gửi thông tin cập nhật về định tuyến ra một cổng nào đó bằng lệnh passive – interface.

GAD(config- router)#passive- interface Fa0/0.

- RIP là giao thức broadcast. Do đó, khi muốn chạy RIP trong mạng non-broadcast như Frame Relay thì ta cần phải khai báo các router RIP lắng nghe bằng lệnh sau:

GAD(config- router) # neighbor ip address

- Phần mềm Cisco IOS mặc nhiên nhận gói thông tin của cả RIP phiên bản 1 và 2 nhưng chỉ gửi đi gói thông tin bằng RIP phiên bản 1. Nhà quản trị mạng có thể cấu hình cho router chỉ gửi và nhận gói phiên bản 1 hoặc là chỉ gửi gói phiên bản 2...bằng các lệnh sau:

```
GAD(config- router) # version {1/2}
GAD(config- if) # ip rip send version 1
GAD(config- if) # ip rip send version 2
GAD(config- if) # ip rip send version 1 2
GAD(config- if) # ip rip receive version 1
GAD(config- if) # ip rip receive version 2
GAD(config- if) # ip rip receive version 1 2
```

2.5 Kiểm tra cấu hình RIP

- Có nhiều lệnh có thể sử dụng để kiểm tra cấu hình RIP có đúng hay không. Trong đó hai lệnh thường được sử dụng nhiều nhất là **Show ip route** và **show ip protocols**.

- Lệnh **show ip protocols** sẽ hiển thị các giao thức định tuyến IP đang được chạy trên router. Kết quả hiển thị của lệnh này có thể giúp kiểm tra được phần lớn cấu hình của RIP nhưng chưa phải là đầy đủ, toàn bộ. Sau đây là một số điểm cần chú ý kiểm tra:

- Có đúng là giao thức định tuyến RIP đã được cấu hình hay không.
- RIP được cấu hình để gửi và nhận thông tin cập nhật trên các cổng vào, có chính xác hay không.
- Các địa chỉ mạng được khai báo trên router để chạy RIP có đúng hay không.

```
GAD# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 5
seconds
  Invalid after 180 seconds, hold down 180, flushed
after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: Rip
  Default version control: send version 1, receive any
version
```

Interface	Send	Recv	Triggered	RIP	Key-chain
FastEthernet0/0	1	1 2			
Ser1a10/0	1	1 2			

```
Routing for Network:
  192.168.1.0
  192.168.2.0
```

Xác định RIP được cấu hình

Xác định mạng đang chạy

Giao diện RIP được xác định

Hình 7. 10: Lệnh show ip protocols

- Lệnh **show ip router** được sử dụng để kiểm tra xem những đường đi mà router học được từ các router RIP láng giềng có được cài đặt vào bảng định tuyến không trên. Trên kết quả hiển thị bảng định tuyến, kiểm tra các đường có đánh dấu bằng chữ “R” ở đầu dòng là những đường mà router học được từ các router RIP láng giềng. cũng nên nhớ rằng các router luôn có một khoảng thời gian để hội tụ với nhau, do đó các thông tin mới có thể chưa được hiển thị ngay trên bảng định tuyến được. Ngoài ra còn có một số lệnh khác mà có thể sử dụng để kiểm tra cấu hình RIP :

- Show interface interface.
- Show ip interface interface.
- Show running –config

```
GAD# show ip route
Codes: c - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type2
       E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
       i - IS-IS, LI - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter
area
       * - candidate default, u - per-user
static route, o - ODR
       p - periodic download static route

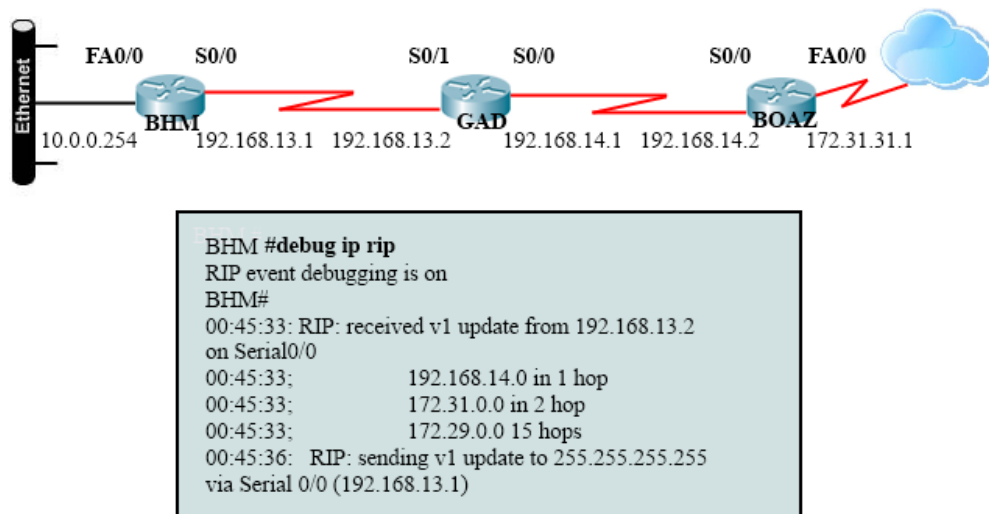
Gateway of last resort is not set
```

Hình 7. 11: Lệnh show ip router

2.6 Xử lý sự cố về hoạt động cập nhật của RIP

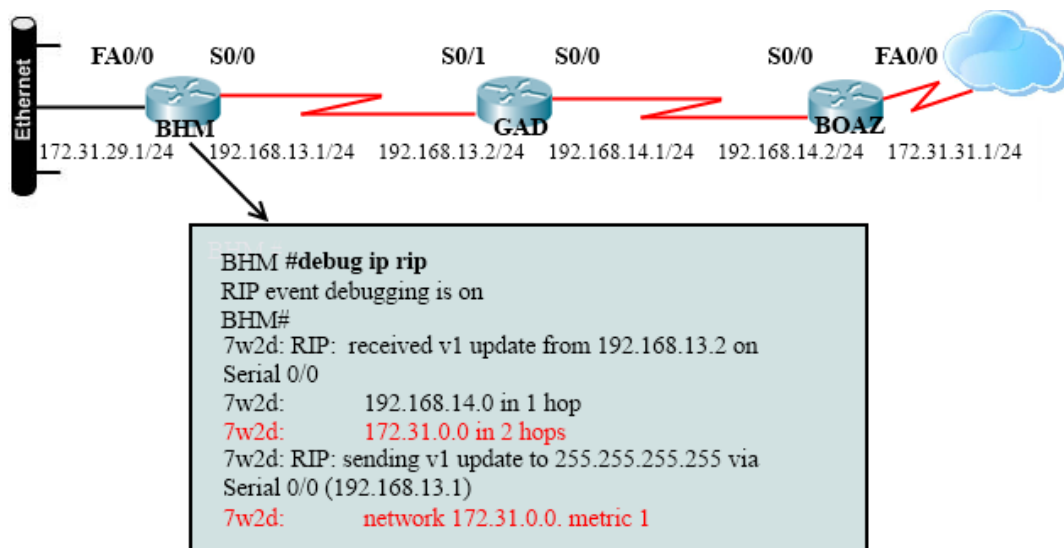
- Hầu hết các lỗi cấu hình RIP đều do khai báo câu lệnh network sai, subnet không liên tục hoặc là do split horizon. Lệnh có tác dụng nhất trong việc tìm lỗi của RIP trong hoạt động cập nhật là lệnh debug ip rip.

- Lệnh debug ip rip sẽ hiển thị tất cả các thông tin định tuyến mà RIP gửi và nhận. Ví dụ trong hình 7.11 cho thấy kết quả hiển thị của lệnh debug ip rip. Sau khi nhận được thông tin cập nhật, router sẽ xử lý thông tin đó rồi sau đó gửi thông tin mới vừa cập nhật ra các cổng. Trong hình 7.11 cho thấy router chạy RIP phiên bản 1 và RTP gửi cập nhật theo kiểu broadcast (địa chỉ broadcast 255.255.255.255). Số trong ngoặc đơn là địa chỉ nguồn của gói thông tin cập nhật RIP.

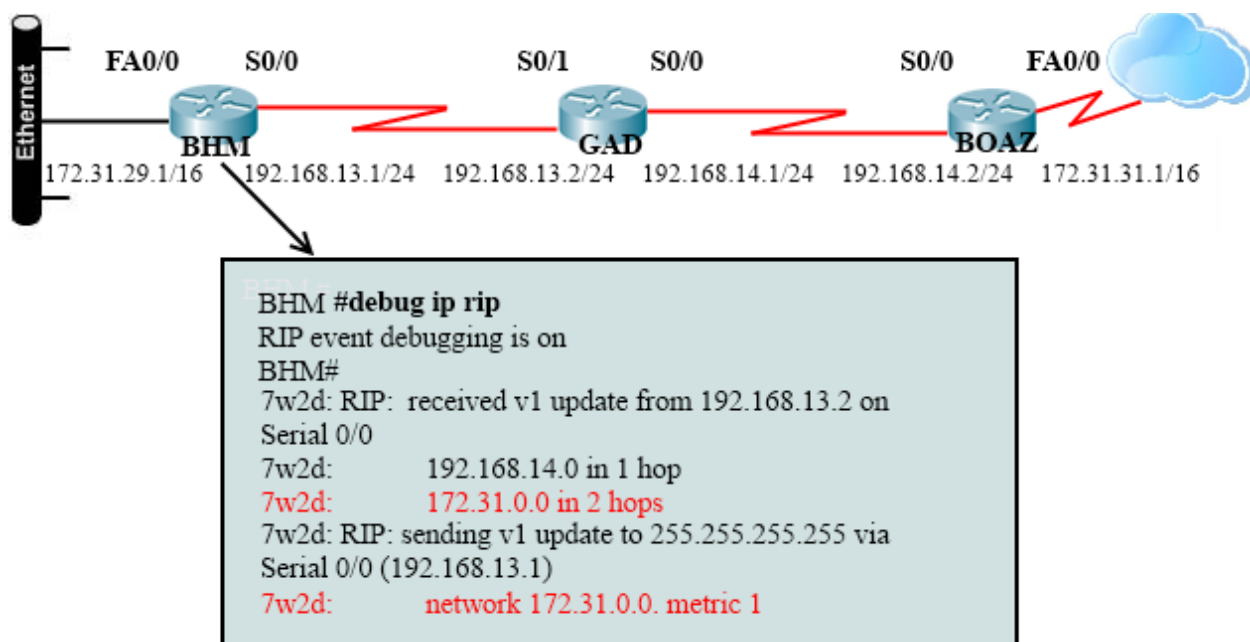


Hình 7. 12: lệnh debug ip rip

- Có rất nhiều điểm quan trọng mà cần chú ý trong kết quả hiển thị của lệnh debug ip rip. Một số vấn đề phải ví dụ như subnet không liên tục hay trùng subnet, có thể phát hiện được nhờ lệnh này. Trong những trường hợp như vậy sẽ thấy là cùng một mạng đích nhưng router gửi thông tin đi thì mạng đích đó lại có thông số định tuyến thấp hơn so với khi router nhận vào trước đó.



Hình 7. 13: Subnet không liên tục



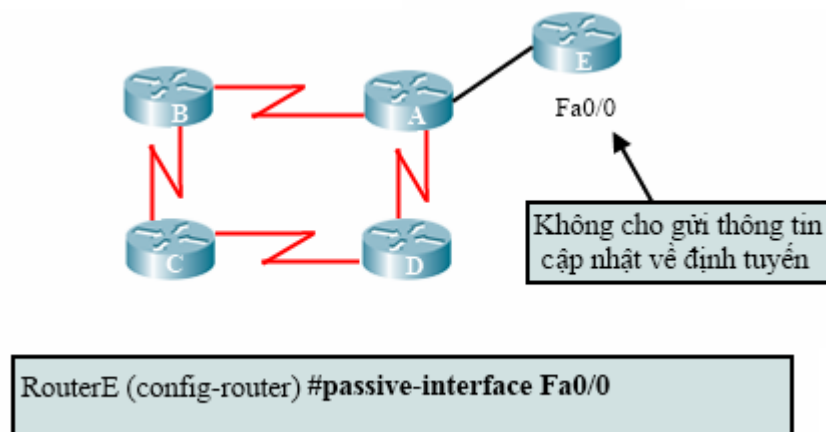
Hình 7. 14: Trùng Subnet

- Ngoài ra còn một số lệnh có thể sử dụng để xử lý sự cố của RIP:
 - + Show ip database.
 - + Show ip protocols(summary).
 - + Show ip route.
 - + Debug ip rip{ events}.
 - + Show ip interface brief.

2.7 Ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp

- Router có thể thực hiện chọn lọc thông tin định tuyến khi cập nhật hoặc khi gửi thông tin cập nhật. Đối với router sử dụng giao thức định tuyến theo vector khoảng cách, cơ chế này có tác dụng vì router định tuyến dựa trên các thông tin định tuyến nhận được từ các router láng giềng. Tuy nhiên, đối với các router sử dụng giao thức định tuyến theo trạng thái đường liên kết thì cơ chế trên không hiệu quả vì các giao thức định tuyến này quyết định chọn đường đi dựa trên cơ sở dữ liệu về trạng thái các đường liên kết chứ không dựa vào thông tin định tuyến nhận được. Chính vì vậy mà cách thực hiện để ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp được đề cập dưới đây chỉ sử dụng cho các giao thức định tuyến theo vector khoảng cách như RIP, IGRP thôi.

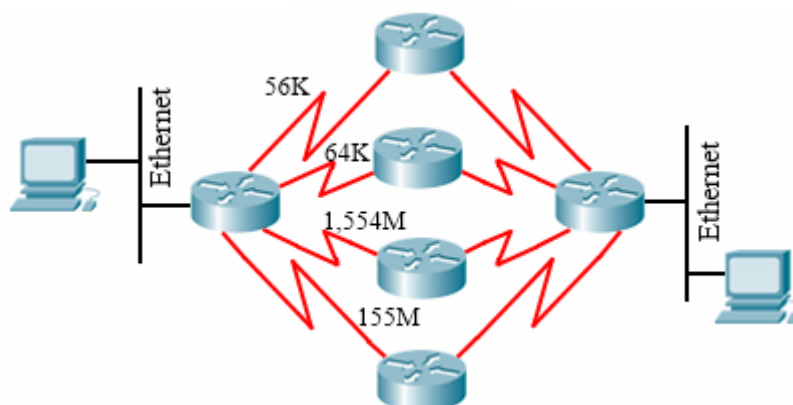
- có thể sử dụng lệnh passive interface để ngăn không cho router gửi thông tin cập nhật về định tuyến ra một cổng nào đó. Làm như vậy thì sẽ ngăn được hệ thống mạng khác học được các thông tin định tuyến trong hệ thống của mình. Đối với RIP và IGRP, lệnh passive interface sẽ làm cho router ngưng việc gửi thông tin cập nhật về định tuyến cho một router láng giềng nào đó, nhưng router vẫn tiếp tục lắng nghe và nhận thông tin cập nhật từ router láng giềng đó.



Hình 7. 15: Lệnh passive interface

2.8 Chia tải với RIP

- Router có thể chia tải ra nhiều đường khi có nhiều đường tốt đến cùng một đích. có thể cấu hình bằng tay cho router chia tải ra các đường hoặc là các giao thức định tuyến động có thể tự tính toán để chia tải.
- RIP có khả năng chia tải ra tối đa là sáu đường có chi phí bằng nhau, còn mặc định thì RIP chỉ chia ra làm 4 đường. RIP thực hiện chia tải bằng cách sử dụng lần lượt và luân phiên từng đường.
- Trong hình 7.15 là ví dụ cho ta thấy RIP chia tải ra 4 đường có chi phí bằng nhau. Đầu tiên router bắt đầu với đường số 1 rồi sau đó lần lượt các đường 2-3-4 rồi 1-2- 3-4-1 và cứ tiếp tục luân phiên như vậy. Vì thông số định tuyến của RIP là số lượng hop lên các đường này được xem là như nhau, RIP không cần quan tâm đến tốc độ của mỗi đường. Do đó đường 56kbps cũng giống như đường 155Mbps.



Hình 7. 16: RIP chia tải ra 4 đường có chi phí bằng nhau

- Trong hình 7.16 là ví dụ về kết quả hiển thị của lệnh show ip route. Trong đó, thấy có hai phần, mỗi phần mô tả về một đường. Trong phần mô tả về đường thứ hai có dấu(*) ở đầu dòng. Dấu (*) này cho biết con đường này là con đường kế tiếp sẽ được sử dụng.

```

RouterC#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Last update from 192.168.4.2 on FastEthernet0/0,
  00:00:18 ago
  Routing Descriptor Blocks:
    192.168.4.1, from 192.168.4.1, 00:02:45 ago, via
    FastEthernet0/0
      Route metric is 1, traffic share count is 1
    192.168.4.2, from 192.168.4.2, 00:00:18 ago,
    via FastEthernet0/0
      Route metric is 1, traffic share count is 1

```

Hình 7. 17: Lệnh show ip route

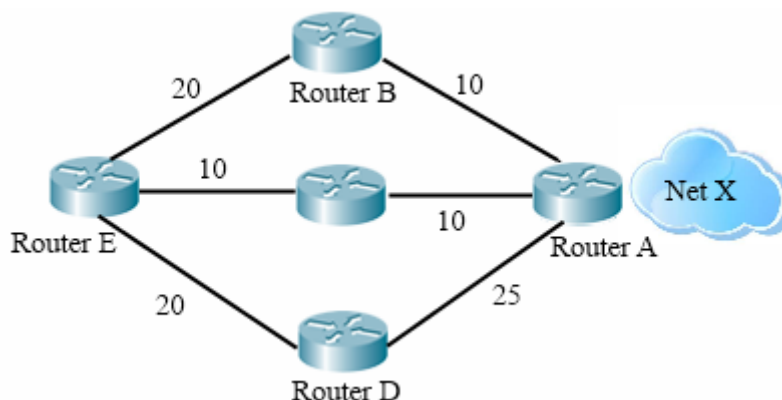
2.9 Chia tải cho nhiều đường

- Router có khả năng chia tải ra nhiều đường để chuyển các gói dữ liệu đến cùng mục đích. Chúng ta có thể cấu hình bằng tay cho router thực hiện chia tải hoặc là các giao thức định tuyến động như RIP, IGRP, EIGRP và OSPF sẽ tự động tính toán.

- Khi router nhận được thông tin cập nhật về nhiều đường khác nhau đến cùng một đích thì router sẽ chọn đường nào có chỉ số tin cậy (Administrative distance) nhỏ nhất để đặt vào bảng định tuyến. Trong trường hợp các đường này có cùng chỉ số tin cậy thì router sẽ chọn đường nào có chi phí thấp nhất hoặc là đường nào có thông số định tuyến nhỏ nhất. Mỗi giao thức định tuyến sẽ có cách tính chi phí khác nhau và cần phải cấu hình các chi phí này để router thực hiện chia tải.

- Khi router có nhiều đường có cùng chỉ số tin cậy và cùng chi phí đến cùng một đích thì router sẽ thực hiện việc chia tải. Thông thường thì router có khả năng chia tải đến 6 đường có cùng chi phí (giới hạn tối đa số đường chia tải là phụ thuộc vào bảng định tuyến của Cisco IOS), tuy nhiên một số giao thức định tuyến nội (IGP) có thể có giới hạn riêng. Ví dụ như EIGRP chỉ cho phép tối đa là 4 đường.

- Mặc định thì hầu hết các giao thức định tuyến IP đều chia tải ra 4 đường. Đường cố định thì chia tải ra 6 đường. Chỉ riêng BGP là ngoại lệ, mặc định của BGP là chỉ cho phép định tuyến 1 đường đến 1 đích.



Hình 7. 18: router có thể chia tải là từ 1 đến 6 đường

- Số đường tối đa mà router có thể chia tải là từ 1 đến 6 đường. Để thay đổi số đường tối đa cho phép sử dụng lệnh sau:

Router(config-router)#maximum-paths[number].

- IGRP có thể chia tải lên tối đa là 6 đường. RIP dựa vào số lượng hop để chọn đường chia tải, trong khi IGRP thì dựa vào bảng thông để chọn đường chia tải.

- Ví dụ như hình 7.17, có ba đường đến mạng X.

- Từ E qua B qua A, thông số định tuyến là 30.
- Từ E qua C qua A, thông số định tuyến là 20.
- Từ E qua D qua A, thông số định tuyến là 45.

- Router E sẽ chọn đường thứ 2 vì đường E –C-A có thông số định tuyến 20 là nhỏ nhất.

- Khi định tuyến IP, Cisco IOS có hai cơ chế chia tải là: chia tải theo gói dữ liệu và chia tải theo địa chỉ đích. Nếu router chuyển mạch theo tiến trình thì router sẽ chia gói dữ liệu ra các đường. Cách này gọi là chia tải theo gói dữ liệu. Còn nếu router chuyển mạch nhanh thì router sẽ chuyển tất cả gói dữ liệu đến cùng mục đích ra một đường. Các gói dữ liệu đến host khác nhưng trong cùng một mạng đích thì sẽ tải ra đường kế tiếp. Cách này gọi là chia tải theo địa chỉ đích.

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

Hình 7. 19: router sẽ sử dụng đường mặc định

2.10 Tích hợp đường cố định với RIP

- Đường cố định là đường do người quản trị cấu hình cho router chuyển gói tới mạng đích theo đường mà mình muốn. Mặt khác, lệnh để cấu hình đường cố định cũng được sử dụng để khai báo cho đường mặc định. Trong trường hợp router không tìm thấy đường nào trên bảng định tuyến để chuyển gói đến mạng đích thì router sẽ sử dụng đường mặc định.

- Router chạy RIP có thể nhận được thông tin về đường mặc định từ những thông tin cập nhật của các router RIP láng giềng khác. Hoặc là bản thân router

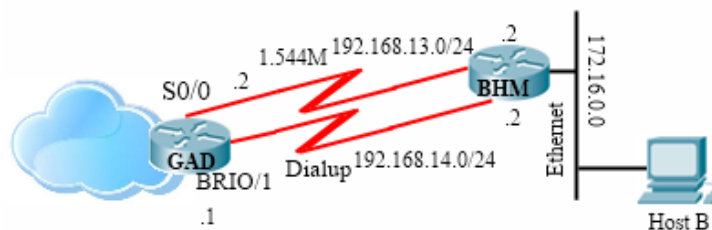
được cấu hình đường mặc định sẽ cập nhật thông tin định tuyến này cho các router khác.

- có thể xóa đường cố định bằng lệnh `no ip route`. Người quản trị mạng có thể cấu hình đường cố định bên cạnh định tuyến động. Mỗi một giao thức định tuyến động có 1 chỉ số tin cậy(AD). Người quản trị mạng có thể cấu hình một đường cố định tới cùng mạng đích với đường định tuyến động nhưng với chỉ số AD lớn hơn chỉ số AD của giao thức định tuyến động tương ứng. Khi đó đường định tuyến động có chỉ số AD nhỏ hơn lên luôn luôn được router chọn lựa trước. Khi đường định tuyến động bị sự cố không sử dụng được nữa thì router sẽ sử dụng tới đường định tuyến cố định để chuyển gói đến mạng đích.

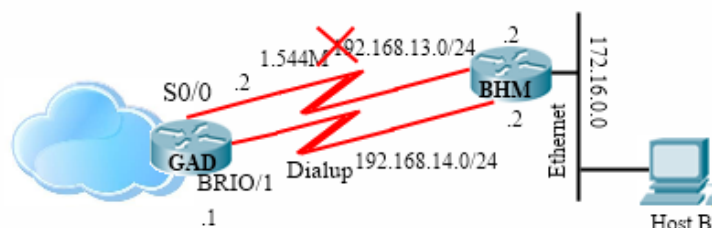
- Nếu cấu hình đường cố định chỉ ra một cổng mà RIP cũng chạy trên cổng đó thì RIP sẽ gửi thông tin cập nhật về đường cố định này cho toàn bộ hệ thống mạng. Vì khi đó, đường cố định đó được xem như là kết nối trực tiếp vào router lên nó không còn bản chất là một đường cố định nữa. Nếu cấu hình đường cố định chỉ ra một cổng mà RIP không chạy trên cổng đó thì RIP sẽ không gửi thông tin cập nhật về đường cố định đó, trừ khi phải cấu hình thêm lệnh `redistribute static` cho RIP.

- Khi một cổng giao tiếp bị ngắt thì tất cả các đường cố định chỉ ra cổng đó đều bị xóa bởi bảng định tuyến. Tương tự như vậy khi router không còn xác định được trạm kế tiếp trên đường cố định cho gói dữ liệu tới mạng đích thì đường cố định đó cũng sẽ bị xóa khỏi bảng định tuyến.

- Trong hình 7.19 và 7.20 chúng ta thấy khi đường định tuyến động của RIP bị sự cố thì đường cố định mà ta đã cấu hình cho router GAD được sử dụng thay thế. Đường cố định như vậy được gọi là đường cố định dự phòng. Như trong ví dụ này chúng ta thấy là đường cố định được cấu hình với chỉ số AD là 130 lớn hơn chỉ số AD của RIP (120). Bên cạnh đó, nên nhớ là trên router BHM cũng cần cấu hình đường mặc định tương ứng.



Hình 7. 20: Cấu hình chỉ số AD



Hình 7. 21: Cấu hình chỉ số AD khi bị sự cố

2.11 Đặc điểm của IGRP

- IGRP là một giao thức định tuyến nội và định tuyến theo vector khoảng cách. Giao thức định tuyến vector khoảng cách chọn lựa đường đi bằng cách so sánh vector khoảng cách. Router chạy giao thức định tuyến theo vector khoảng cách thực hiện bằng định tuyến theo định kỳ cho các router láng giềng. Dựa vào thông tin cập nhật, router thực hiện 2 nhiệm vụ sau :

- Xác định mạng đích mới.
- Cập nhật sự cố về đường đi trên mạng.

- IGRP là giao thức định tuyến theo vector khoảng cách do Cisco phát triển nên. IGRP thực hiện cập nhật theo chu kỳ 90 giây/lần và chỉ gửi thông tin cập nhật trong phạm vi một hệ tự quản. Sau đây là các đặc điểm chính của IGRP:

- Khả năng thích ứng với các cấu trúc mạng phức tạp và không xác định.
- Khả năng linh hoạt với các đặc tính băng thông và độ trễ khác nhau.
- Khả năng mở rộng cho hệ thống mạng lớn.

- Mặc định thì IGRP sử dụng băng thông và độ trễ làm thông số định tuyến. Ngoài ra IGRP còn có thể cấu hình để sử dụng nhiều thông số khác để định tuyến. Sau đây là các thông số mà IGRP có thể sử dụng để định tuyến:

- Băng thông.
- Độ trễ.
- Độ tải.
- Độ tin cậy

2.12 Kiểm tra cấu hình IGRP

- Để kiểm tra xem IGRP đã được cấu hình đúng chưa dùng lệnh show ip route và kiểm tra các đường của IGRP được đánh dấu bằng chữ "I" ở đầu dòng.

- Ngoài ra còn các lệnh sau có thể sử dụng để kiểm tra cấu hình IGRP:

- Show interface interface
- Show running-config
- Show running-config interface interface
- Show running-config | begin interface interface
- Show running-config | begin igrp
- Show ip protocols

- Để kiểm tra xem cổng Ethernet đã được cấu hình đúng chưa thì dùng lệnh show interface fa0/0.

- Để kiểm tra IGRP đã được chạy trên router chưa thì dùng lệnh show ip protocols.

2.13 Xử lý sự cố của IGRP

- Phần lớn các sự cố của IGRP là do khai báo sai lệnh network ,địa chỉ mạng IP không liên tục, khai báo số AS sai .

```
RouterA#debug ip igrp events
IGRP event debugging id on

00:21:38: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:21:38: IGRP: Update contains 0 interior, 2
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 1
```

Hình 7. 22: Lệnh Debug ip igrp events

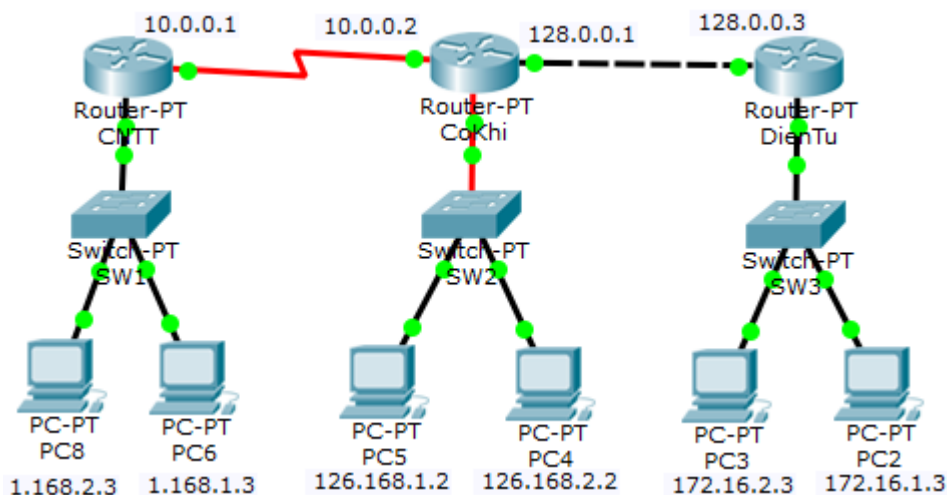
- Sau đây là các lệnh được sử dụng để tìm sự cố của IGRP :

- Show ip protocols
- Show ip route
- Debug ip igrp events
- Debug ip igrp transactions
- Ping
- Traceroute

3.BÀI TẬP THỰC HÀNH 7.1

3.1.Mô hình

- Cho mô hình mạng như hình 7.21:



Hình 7. 23: Mô hình PC kết nối Router

3.2.Yêu cầu

Cấu hình RIP để 3 router CNTT, CoKhi và DienTu thông mạng với nhau.

3.3.Chuẩn bị:

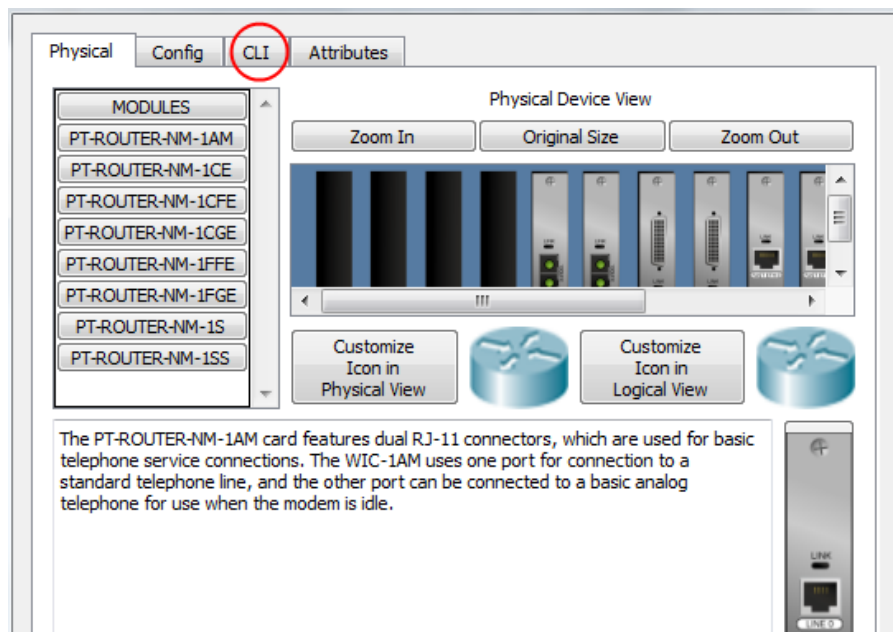
Bảng 7. 1: chuẩn bị phần mềm cài đặt, máy tính, router, swith thực hành bài tập 7.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	6	
3	Router ảo	Cái	3	
4	Swicth ảo	Cái	3	

3.4.Các bước thực hành:

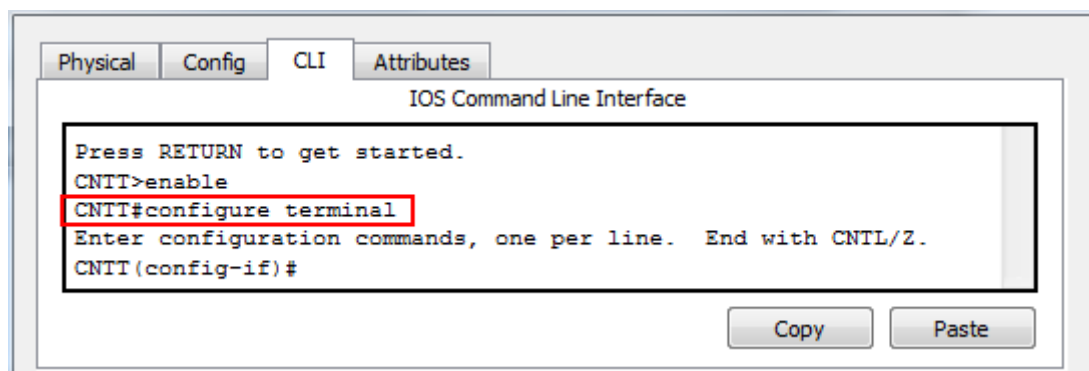
Bước 1: Đầu tiên ta cấu hình cho Router CNTT trước:

- Từ giao diện Physical ta chuyển sang tab CLI .



Hình 7. 24: Chuyển sang tab CLI

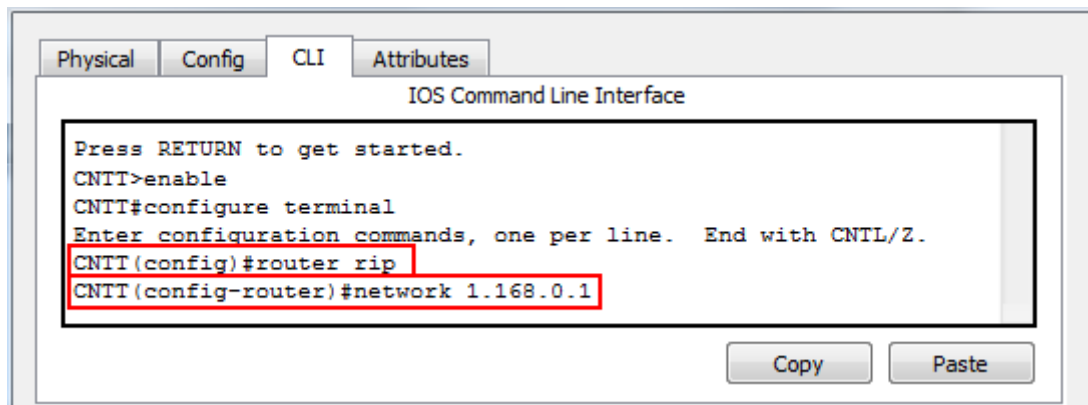
Bước 2: Sau đó gõ lệnh **configure terminal** để chuyển sang chế độ toàn cục.



Hình 7. 25: Chuyển sang chế độ toàn cục

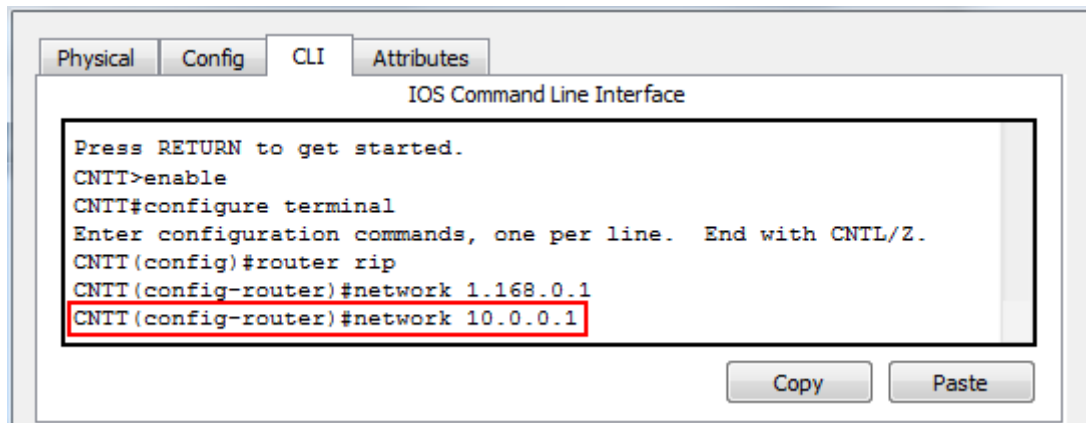
- Gõ tiếp lệnh **router rip** để chuyển sang chế độ cấu hình rip.

- Nhập lệnh **network** <địa chỉ ip của cổng FastEthernet 0/0> như hình 7.25.



Hình 7. 26: Cấu hình RIP cổng FastEthernet 0/0

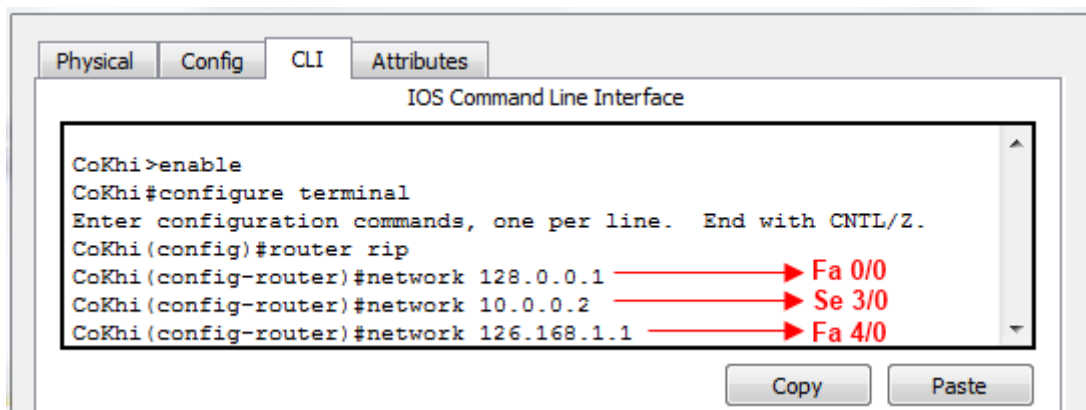
Bước 3: Nhập tiếp lệnh **network** <địa chỉ ip của cổng Serial 2/0>



Hình 7. 27: Cấu hình RIP cổng Serial 2/0

Bước 4: Vào Router CoKhi tương tự như vào Router CNTT

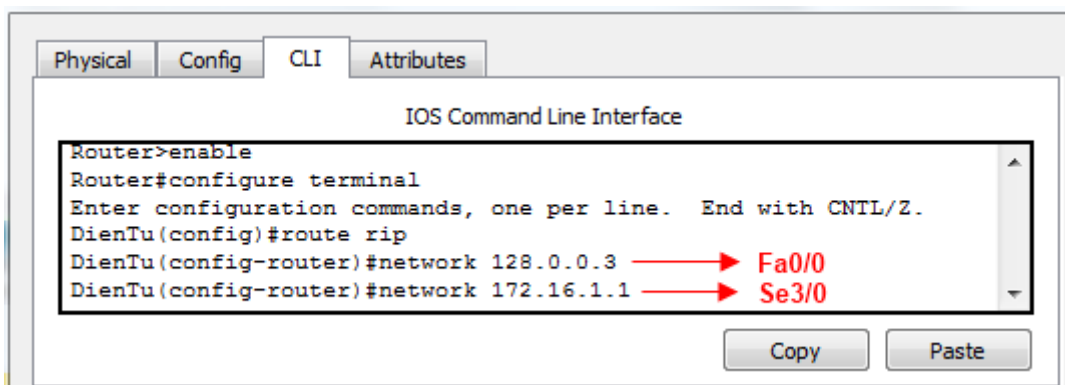
- Ta nhập lệnh Network cho các cổng Fa 0/0, Se 3/0, Fa 4/0 của RouterCoKhi



Hình 7. 28: Cấu hình RIP cho RouterCoKhi

Bước 5: Vào Router DienTu tương tự như 2 Router trước

- Ta nhập lệnh Network cho các cổng Fa 0/0, Se 3/0 của RouterDienTu



Hình 7. 29: Cấu hình RIP cho RouterDienTu

3.5.Những sự cố thường gặp

Bảng 7. 2: những sự cố thường gặp của bài tập 7.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không kết nối được PC với router	Chọn sai router	Chọn router CNTT và bật chế độ mở
Không nhập được địa chỉ IP	Chọn sai máy server	Chọn lại máy server và đặt lại địa chỉ IP
Không cấu hình được chế độ toàn cục	Chưa cập nhật	Lưu và cập nhật
Không cấu hình được giao thức định tuyến	Đặt sai địa chỉ IP	Kiểm tra đặt lại địa chỉ IP và quan sát quá trình định tuyến

3.6.Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

3.7.Đánh giá các bước thực hành

Bảng 7. 3: đánh giá các bước thực hành bài tập 7.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1:Cấu hình cho Router CNTT	Chọn đúng router			

	trước				
2	Bước 2:Nhập lệnh configure terminal để chuyển sang chế độ toàn cục	Nhập đúng lệnh			
3	Bước 3:Nhập tiếp lệnh network <địa chỉ ip của cổng Serial 2/0>	Chọn đúng cổng			
4	Bước 4:Vào Router CoKhi tương tự như vào Router CNTT	Chọn đúng router			
5	Bước 5:Vào Router DienTu tương tự như 2 Router trước	Nhập đúng dòng lệnh và đúng địa chỉ IP			

4.TÓM TẮT NỘI DUNG

- Giao thức định tuyến theo vector khoảng cách thực hiện bảo trì thông tin định tuyến như thế nào.
- Cơ chế định nghĩa giá trị tối đa để tránh đếm vô hạn.
- Tránh vòng lặp bằng split horizon, cơ chế cập nhật tức thời, bằng thời gian holddown.
- Ngăn không cho router gửi thông tin cập nhật về định tuyến ra một cổng .
- Chia tải ra nhiều đường .
- Tiến trình RIP, cấu hình RIP.
- Sử dụng lệnh ip classless.
- Những vấn đề thường gặp khi cấu hình RIP.
- Đặc điểm của IGRP.
- Sự chuyển đổi từ RIP sang IGRP.
- Kiểm tra cấu hình IGRP.
- Xử lý sự cố của IGRP.

5.CÂU HỎI VÀ BÀI TẬP

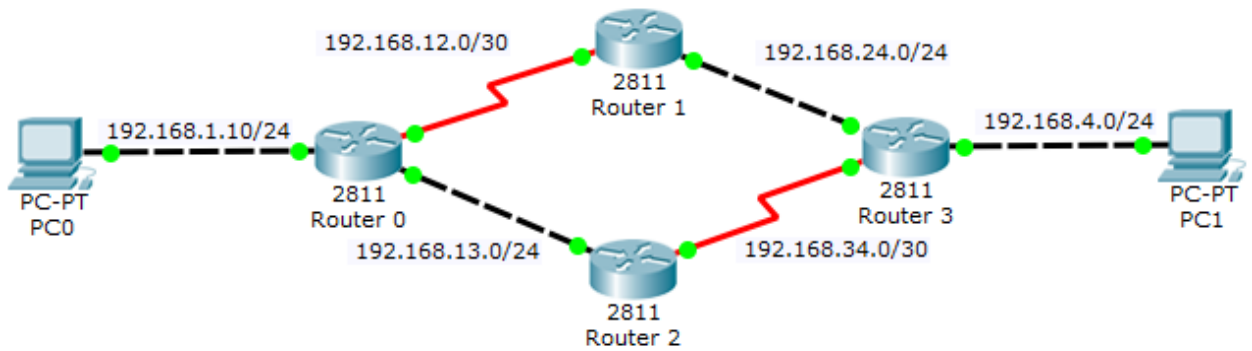
Câu hỏi:

Câu 1: Trình bày Cơ chế định nghĩa giá trị tối đa trong định tuyến theo vector khoảng cách?

Câu 2: Trình bày tiến trình của RIP?

Bài tập:

Cho mô hình mạng như hình :



- Cấu hình định tuyến RIPv2 cho Router.
- Thay đổi thời gian holddown trong cấu hình RIP.

BÀI 8: THÔNG điệp ĐIỀU KHIỂN VÀ BÁO LỖI CỦA TCP/IP

Mã bài MD 28-08

Thời gian: 5 giờ

I. MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Trình bày ICMP;
- Xác định cấu trúc thông điệp ICMP;
- Xác định loại thông điệp báo lỗi ICMP;
- Xác định thông điệp điều khiển ICMP;
- Xác định được các loại thông điệp điều khiển ICMP được sử dụng trong mạng;
- Thực hiện các thao tác an toàn với máy tính;

II. NỘI DUNG CHÍNH

1. Tổng quát về thông điệp báo lỗi của TCP/IP Cách thức.

1.1 Giao thức thông điệp điều khiển Internet (ICMP)

- IP là một phương thức truyền dữ liệu không tin cậy trên mạng. Nó là một giao thức tự nỗ lực tối đa để truyền dữ liệu tới đích. Trong đó, IP không hề có một cơ chế nào để xác nhận là dữ liệu đã đến đích. Nếu một thiết bị trung gian trên đường đi như router chẳng hạn bị sự cố, hay là thiết bị đích không kết nối vào mạng nên dữ liệu không truyền tới đích thì IP không hề có cơ chế nào để thông báo cho người gửi biết là quá trình truyền dữ liệu đã bị sự cố. Giao thức thông điệp điều khiển Internet (ICMP) là một giao thức của bộ TCP/IP đã bổ sung cho khiếm khuyết này của IP. ICMP không khắc phục được sự không tin cậy của IP. ICMP chỉ đơn giản là phát đi các thông điệp để thông báo về sự cố.

1.2 Truyền thông điệp ICMP

- Thông điệp ICMP được đóng gói giống như các dữ liệu khác khi truyền đi bằng IP. Hình 8.1 cho thấy dữ liệu của ICMP được đóng gói trong gói IP như thế nào.

- Thông điệp ICMP cũng được truyền đi như các gói dữ liệu khác cho nên nó cũng có thể gặp sự cố. Điều này dẫn tới một vấn đề là nếu một thông điệp báo lỗi gặp sự cố thì sẽ làm phát sinh thêm các thông điệp báo lỗi nữa và điều này làm cho mạng càng bị nghẽn hơn khi sự cố vốn đã xảy ra và còn đang tồn tại trên mạng. Chính vì vậy, các thông điệp báo lỗi của ICMP sẽ không tạo thêm các thông điệp báo lỗi cho chính nó. Như vậy thì các thông điệp báo lỗi cũng có khả năng là không bao giờ đến được máy nguồn của gói dữ liệu.

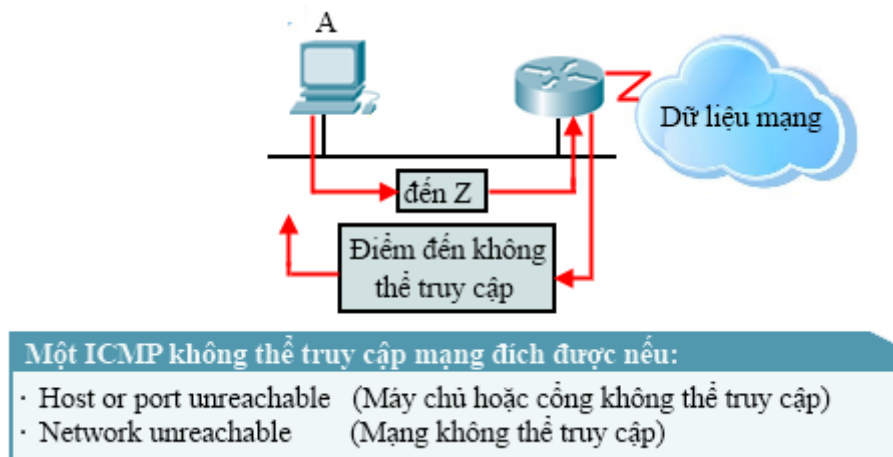
Frame Header	Datagram Header	ICMP Header	ICMP Data
Frame Header	Datagram Header	Datagram Data Area	
Frame Header	Frame Data Area		

Hình 8. 1: Thông điệp ICMP

1.3 Mạng không đến được

- Để thực hiện được việc thông tin liên lạc trên mạng thì các điều kiện cơ bản cần phải có đủ. Trước tiên là thiết bị gửi và nhận dữ liệu phải được cấu hình đúng bộ giao thức TCP/IP. Việc này bao gồm cài đặt bộ giao thức TCP/IP và cấu hình địa chỉ IP, subnet mask cho thiết bị. Ngoài ra cần phải khai báo Default gateway nếu thiết bị cần truyền dữ liệu ra ngoài phạm vi cục bộ. Thứ hai là các thiết bị trung gian phải thực hiện việc định tuyến đúng để chuyển gói từ nguồn đến đích. Router là thiết bị thực hiện nhiệm vụ này. Do đó router phải được cấu hình bộ TCP/IP cho các cổng giao tiếp và sử dụng giao thức định tuyến thích hợp.

- Nếu 2 điều kiện trên không được đáp ứng thì hệ thống mạng không thể thực hiện thông tin liên lạc được. Ví dụ như khi một thiết bị gửi dữ liệu đến một địa chỉ IP không tồn tại hoặc là thiết bị đích đã bị ngắt kết nối ra khỏi mạng. Router cũng là nguyên nhân của sự cố nếu cổng giao tiếp trên router bị ngắt hoặc router không có thông tin cần thiết để tìm ra đường tới mạng đích. Những trường hợp như vậy đều được xem là mạng đích không đến được. Hình 8.2 minh họa cho trường hợp router không thể gửi gói dữ liệu đến đích do router không biết đường đến mạng đích, router gửi thông điệp ICMP về cho máy nguồn để thông báo là mạng đích không đến được.

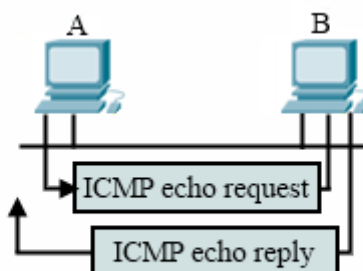


Hình 8. 2: router gửi thông điệp ICMP

1.4 Sử dụng lệnh ping để kiểm tra xem địa chỉ đích có đến được hay không

- Giao thức ICMP có thể được sử dụng để kiểm tra xem có đến được một địa chỉ nào đó hay không. ICMP sẽ gửi thông điệp echo request đến máy đích. Nếu máy đích nhận được echo request thì sẽ trả lời lại thông điệp echo reply cho máy nguồn. Nếu máy nguồn nhận được echo reply thì điều đó khẳng định là máy đích có thể đến được bằng giao thức IP.

- Lệnh ping khởi tạo các thông điệp echo request. Ví dụ như hình 8.3 và 8.4, chúng ta sử dụng lệnh ping với địa chỉ IP đích. Lệnh ping gửi đi 4 gói echo request và nhận về 4 gói echo reply xác nhận kết nối IP giữa 2 thiết bị hoạt động tốt.



Lưu lượng được tạo ra bởi lệnh ping

Hình 8. 3: : Lệnh ping gửi đi 4 gói echo request

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Hình 8. 4: Lệnh ping địa chỉ IP

1.5 Phát hiện đường dài quá giới hạn

- Gói dữ liệu khi truyền đi trên mạng có thể bị truyền lòng vòng và không bao giờ đến được đích. Điều này có thể xảy ra khi thông tin định tuyến bị sai, ví dụ như 2 router củ gửi một gói dữ liệu qua lại cho nhau vì router này nghĩ rằng router kia mới là trạm kế tiếp đến đích. Giao thức định tuyến có quy trình có quy định giới hạn để xác định mạng đích không đến được. Ví dụ như RIP có số hop giới hạn là 15. Điều này có nghĩa là gói dữ liệu chỉ được phép đi qua tối đa 15 router.

- Khi con đường mà gói dữ liệu đi qua bị lặp vòng hoặc có quá nhiều hop thì khi gói dữ liệu vượt qua giá trị hop tối đa, giá trị Time-to-live (TTL) của gói dữ liệu cũng hết thời gian vì giá trị TTL được cài đặt khớp với số hop tối đa đã được định nghĩa của giao thức định tuyến. Mỗi một gói dữ liệu đều có một giá trị TTL. Mỗi router sau khi xử lý gói dữ liệu sẽ giảm giá trị TTL đi. Khi giá trị TTL bằng 0 thì router sẽ hủy bỏ gói dữ liệu đó. Khi đó ICMP dùng thông điệp

“Time exceeded” để thông báo cho máy nguồn biết là TTL của gói dữ liệu đã bị hết thời gian.

1.6 Thông điệp echo

- Như bất kỳ các loại gói dữ liệu khác, thông điệp ICMP cũng có định dạng riêng. Mỗi một loại thông điệp ICMP có một đặc điểm riêng nhưng tất cả các gói ICMP đều bắt đầu bằng 3 phần:

- + Type
- + Code
- + Checksum

- Phần type cho biết loại thông điệp nào của ICMP được gửi đi. Phần Code cho biết chi tiết hơn về loại thông điệp ICMP. Phần checksum cũng tương tự như trong các loại gói dữ liệu khác, phần này được sử dụng để kiểm tra lỗi cho dữ liệu.

1.7 Thông điệp “Destination Unreachable”

- Không phải lúc nào gói dữ liệu cũng chuyển được đến đích. Ví dụ như hư hỏng phần cứng, cấu hình giao thức không đúng, cổng giao tiếp bị ngắt, thông tin định tuyến sai... là những nguyên nhân có thể gây ra làm cho gói dữ liệu không thể chuyển được tới đích. Trong những trường hợp như vậy thì ICMP gửi thông điệp “Destination Unreachable” cho máy gửi để thông báo là gói dữ liệu không chuyển được tới đích.

- Trong hình 8.5 là cấu trúc của thông điệp “Destination Unreachable”. Giá trị 3 trong phần Type cho biết đây là thông điệp “Destination Unreachable”. Giá trị trong phần Code sẽ cho biết nguyên nhân tại sao không chuyển được gói dữ liệu đến đích. Ví dụ như phần Code có giá trị 0 có nghĩa là mạng đích không đến được.

0	8	16	31
Type (3)	Code (0-12)	Checksum	
Unused (must be zero)			
Internet Header + First 64 Bits of Datagram			
...			

Hình 8. 5: Thông điệp “Destination Unreachable”

- Khi gói dữ liệu được chuyển từ mạng Token-ring ra mạng Ethernet thì thường phải phân mảnh ra thành các gói nhỏ hơn. Nếu gói dữ liệu không cho phép phân mảnh thì gói dữ liệu không thể chuyển ra được, khi đó thông điệp “Destination Unreachable” sẽ được gửi đi. Thông điệp ICMP này cũng được gửi đi khi các dịch vụ liên quan đến IP như FTP, Web không tìm thấy. Điều quan trọng khi xử lý sự cố mạng IP là cần phải hiểu được các nguyên nhân khác nhau tạo nên thông điệp ICMP “Destination Unreachable”.

1.8 Thông báo các loại lỗi khác

- Khi thiết bị xử lý gói dữ liệu không chuyển gói dữ liệu đi được do một số lỗi ở phần Header của gói dữ liệu. Loại dữ liệu này không liên quan gì đến host đích hay mạng đích nhưng nó vẫn làm cho gói dữ liệu không thể chuyển được đến đích. Trong trường hợp này, thông điệp ICMP “Parameter Problem”, Type 12 sẽ được gửi về cho máy nguồn.

- Trong hình 8.6 là cấu trúc của thông điệp “Parameter Problem”. Trong đó có phần Pointer. Khi giá trị Code là 0, phần Pointer cho biết octet nào trong gói dữ liệu bị lỗi.

0	8	16	31
Type (12)	Code (0-12)	Checksum	
Pointer		Unused (must be zero)	
Internet Header + First 64 Bits of Datagram			
...			

Hình 8. 6: Thông điệp “Parameter Problem”

2. Thông điệp điều khiển của TCP/IP.

2.1 Giới thiệu về thông điệp điều khiển

- ICMP là một phần của bộ giao thức TCP/IP. Thực tế là tất cả các hệ thống IP đều phải bao gồm ICMP. Lý do của việc này hết sức đơn giản. Trước hết là IP không có cơ chế nào để đảm bảo là dữ liệu đã được chuyển tới đích, hoàn toàn không thông báo gì cho host biết khi sự cố xảy ra. IP không có cơ chế cung cấp thông điệp thông báo hoặc điều khiển cho host. Và ICMP đã thực hiện việc này cho IP.

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

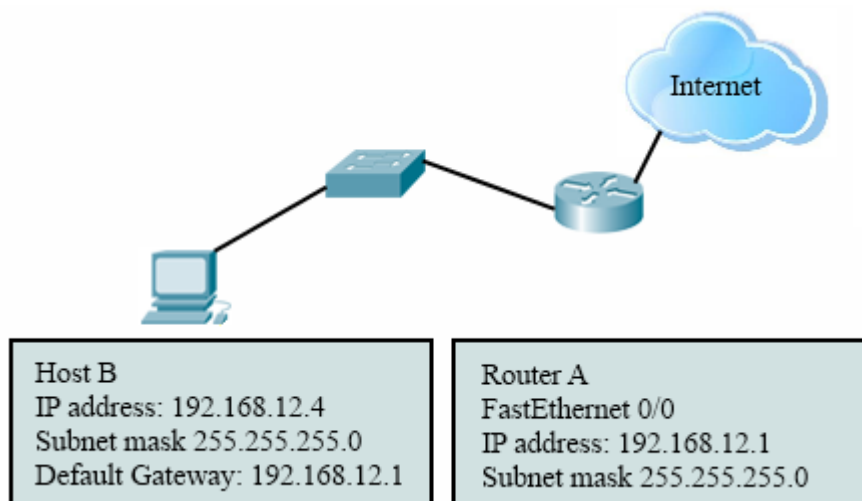
Hình 8. 7: : Một số thông điệp ICMP

- Không giống như thông điệp báo lỗi, thông điệp điều khiển không phải được tạo ra là do mất gói dữ liệu hay do lỗi của quá trình truyền dữ liệu. Mà

các thông điệp điều khiển được dùng để thông báo cho host biết về tình trạng nghẽn mạch trên mạng hay thông báo cho host biết là có một gateway tốt hơn dẫn đến mạng đích... Cũng giống như tất cả các gói ICMP khác, thông điệp điều khiển được đóng gói trong gói IP. ICMP sử dụng gói IP để truyền thông điệp trên mạng. ICMP có rất nhiều loại thông điệp điều khiển khác gặp nhất được thể hiện ở hình 8.7.

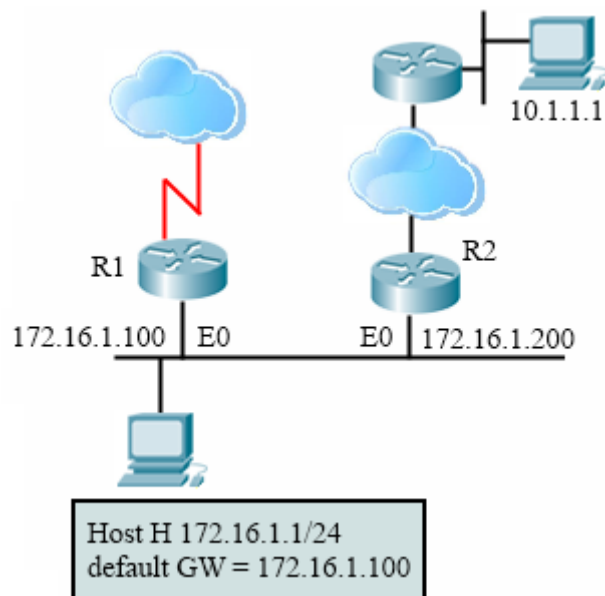
2.2 Thông điệp ICMP redirect/change request

- Thông điệp điều khiển ICMP thường gặp nhất là redirect/change request. Loại thông điệp này được tạo ra bởi gateway mà thông thường đó chính là router. Tất cả các host khi muốn thông tin liên lạc với các mạng IP đều phải được cấu hình default gateway. Default gateway là địa chỉ của một cổng trên router kết nối vào cùng một mạng với host. Như trong hình 8.8, một host được nối vào router và router này có kết nối ra Internet. Host B được cấu hình default gateway là địa chỉ IP của cổng Fa0/0 trên router. Host B sẽ sử dụng địa chỉ IP này để đến các mạng khác. Bình thường host B chỉ kết nối đến một gateway. Tuy nhiên cũng có trường hợp một host kết nối vào mạng 2 hay nhiều router. Trong trường hợp đó, default gateway của host sẽ cần dùng redirect/change request để thông báo cho host biết về một gateway khác tốt hơn để đến một mạng đích nào đó.



Hình 8. 8: Thông điệp ICMP redirect/change request

- Trong hình 8.8 là một ví dụ cho trường hợp cần sử dụng ICMP redirect. Host H gửi dữ liệu cho Host C trong mạng 10.0.0.0/8. Vì mạng đích không kết nối trực tiếp vào Host H nên Host H gửi gói đến default gateway của nó là Router R1. Router R1 tìm trên bảng định tuyến để tìm đường đến mạng 10.0.0.0/8 thì thấy rằng để chuyển gói tới đích router phải gửi gói này ngược trở ra cổng mà nó vừa mới nhận gói dữ liệu vào. Khi đó router R1 sẽ chuyển gói dữ liệu đi và đồng thời gửi thông điệp ICMP redirect/change request tới Host H để thông báo là Host H nên sử dụng Router R2 làm gateway cho tất cả các gói dữ liệu đến mạng 10.0.0.0/8.



Hình 8. 9: Host H nên sử dụng Router R2 làm gateway

- Default gateway chỉ gửi thông điệp ICMP redirect/change request khi gặp các điều kiện sau :
 - + Cổng mà router nhận gói dữ liệu vào cũng chính là cổng mà router sẽ chuyển gói dữ liệu đi.
 - + Địa chỉ IP của máy nguồn là cùng một mạng/ subnet với địa chỉ IP của trạm kế tiếp.
 - + Gói dữ liệu nhận được không phải gửi ngược lại máy nguồn .
 - + Con đường mà router thực hiện thông báo cho host không phải là đường mặc định của router và cũng không phải là của một ICMP redirect nào khác.
 - + Router phải được cấu hình để thực hiện redirect. (Mặc định là Cisco router thực hiện gửi ICMP redirect. có thể dùng lệnh no ip redirect để tắt chức năng này trên một cổng nào đó của router).

2.3 Đồng bộ đồng hồ và ước tính Thời gian truyền dữ liệu

- Bộ giao thức TCP/IP cho phép hệ thống mạng này kết nối với hệ thống mạng khác ở cách nhau rất xa thông qua nhiều hệ thống mạng trung gian. Mỗi một hệ thống mạng có một cơ chế đồng bộ đồng hồ riêng. Do đó khi một host ở mạng khác sử dụng phần mềm cần đồng bộ thời gian để thực hiện liên lạc thì có thể sẽ gặp rắc rối. Thông điệp ICMP Timestamp được thiết kế để giải quyết vấn đề này.
 - Thông điệp ICMP timestamp request cho phép một host hỏi giờ hiện tại trên một máy khác. Máy được hỏi sẽ dùng thông điệp ICMP timestamp reply để trả lời. Phần Type trong thông điệp ICMP timestamp có giá trị là 13 (timestamp request)hoặc 14(timestamp reply). Phần Code luôn có giá trị là 0 vì loại thông điệp này không có gì khác hơn. Phần Originate timestamp là thông tin về giờ hiện tại trên máy gửi ngay trước khi thông điệp ICMP timestamp request được gửi đi .Phần Recive timestamp là thời điểm mà máy đích nhận

được yêu cầu request. Phần Transmit timestamp là thời điểm trên máy trả lời ngay trước khi máy này gửi thông điệp ICMP timestamp reply.

- Tất cả 3 thông số về thời gian trên đều được tính bằng số mili giây tính từ thời điểm nửa đêm theo giờ Quốc tế (Univesal Time -UT).

0	8	16	31
Type (13 or 14)	Code (0)	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

Hình 8. 10: Thông điệp hỏi giờ

2.4 Thông điệp Information request và reply

- Khi người quản trị mạng dùng một địa chỉ IP lớn chia ra thành nhiều subnet, các subnet sẽ có subnet mask tương ứng. Subnet mask được sử dụng để xác nhận các bit của phần Network. Subnet và các bit của thành phần Host trong địa chỉ IP. Nếu một host biết địa chỉ IP của router thì nó gửi yêu cầu tới trực tiếp của router, còn nếu không thì nó sẽ quảng bá yêu cầu của nó. Khi router nhận được yêu cầu này, router sẽ dùng thông điệp Address mask reply để trả lời. Trong thông điệp Address mask reply sẽ có subnet mask chính xác cho host.Ví dụ: một host trong mạng lớp B có địa chỉ IP là 172.16.5.2. Host này không biết subnet mask của mình nên nó broadcast thông điệp Address mask request như sau:

Source address:172.16.5.2

Destination address:255.255.255.255

Protocol :ICMP =1

Type :Address Mask Request =AM1

Code :0

Mask:255.255.255.0

- Router 172.16.5.2 nhận được thông điệp trên và trả lời bằng thông điệp Address mask reply như sau :

Source address:172.16.5.1

Destination address:172.16.5.2

Protocol :ICMP =-1

Type :Address Mask Request =AM2

Code :0

Mask:255.255.255.0

- Cấu trúc của thông điệp Address Mask Request và reply được thể hiện ở hình 8.11. Thông điệp Address Mask Request và reply có cấu trúc hoàn toàn như nhau, chỉ khác nhau giá trị phần Type. Phần Type có giá trị 17 là tương ứng với request, còn giá trị 18 là tương ứng với reply. Phần Identifier và Sequence Number giúp phân biệt reply nào tương ứng với request nào, giá trị hai phần này thường là 0. Phần Checksum được dùng để kiểm tra lỗi cho thông điệp ICMP được tính bắt đầu từ phần Type trở đi.

0	8	16	31
Type (17 or 18)	Code (0)	Checksum	
Identifier		Sequence Number	
Address Mask			
...			

Hình 8. 11: Cấu trúc của thông điệp Address Mask Request và reply

2.5 Thông điệp để tìm router

- Khi có host trong mạng bắt đầu khởi động và host chưa được cấu hình Default gateway thì nó có thể tìm gateway bằng thông điệp Router discovery. Trước tiên, host gửi thông điệp Router solicitation cho tất cả các router bằng cách dùng địa chỉ multicast là 224.0.0.2. Thông điệp này cũng có thể được gửi broadcast để gửi đến được những router không có cấu hình multicast. Khi nhận được thông điệp trên, nếu router không có cấu hình hỗ trợ quá trình này thì router sẽ không trả lời gì hết. Còn nếu router có hỗ trợ quá trình này thì router sẽ trả lời lại bằng thông điệp Router advertisement. Hình 8.12

0	8	16	31
Type (9)	Code (0)	Checksum	
Number of Addresses	Address Entry Size	Lifetime	
Router Address 1			
Preferences Level 1			
Router Address 2			
Preferences Level 2			

Hình 8. 12: Cấu trúc của thông tin điệp Router advertisement

2.6 Thông điệp Router solicitation

- Host gửi thông điệp Router solicitation trong trường hợp bị mất Default gateway. Thông điệp này được gửi multicast và đây chính là bước đầu tiên của quá trình tìm router đã đề cập ở phần 8.12. Router sẽ trả lời lại bằng thông điệp Router Advertisement, trong đó có cung cấp Default gateway cho host.

0	8	16	31
Type (10)	Code (0)	Checksum	
Reserved			

Hình 8. 13: Cấu trúc của thông điệp Router solicitation

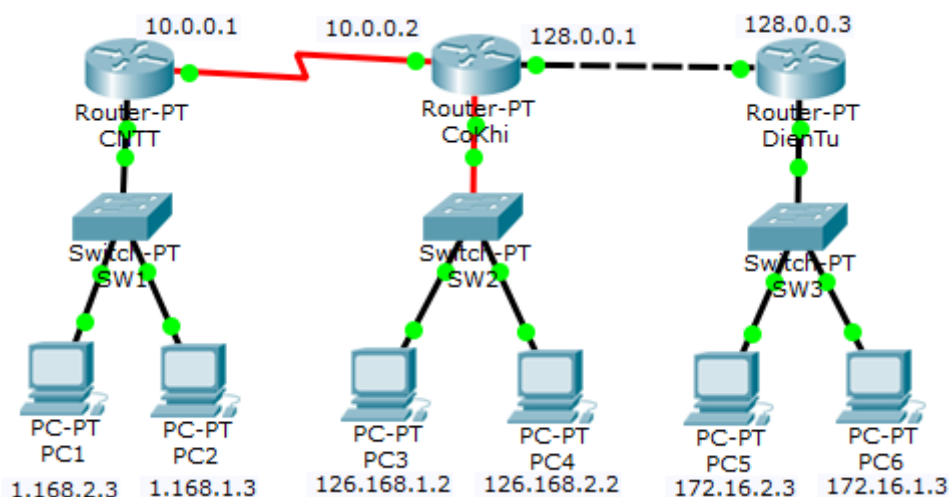
2.7 Thông điệp báo nghẽn và điều khiển luồng dữ liệu

- Nếu có nhiều máy tính cùng lúc truy xuất vào cùng một máy đích thì máy đích có thể bị quá tải. Nghẽn mạch có thể xảy ra khi lưu lượng từ mạng LAN tốc độ cao được truyền ra kết nối WAN có tốc độ thấp hơn. Nếu mạng bị nghẽn quá mức thì các gói dữ liệu sẽ bị hủy bỏ. Thông điệp ICMP source-quence giúp làm giảm lượng dữ liệu bị hủy bỏ. Thông điệp này sẽ được gửi cho máy gửi để yêu cầu máy gửi giảm tốc độ phát gói dữ liệu. Sau khoảng thời gian ngắn, nghẽn mạch được giải tỏa và máy gửi có thể tăng dần tốc độ truyền lên sau khi không còn nhận được thông điệp source-quence nào nữa. Mặc định là đa số các Cisco router không thực hiện gửi thông điệp source-quence vì có thể các thông điệp này còn làm cho tình trạng tắc nghẽn bị tăng thêm.

3.BÀI TẬP THỰC HÀNH 8.1

3.1.Mô hình

- Cho mô hình mạng như hình 8.14:



Hình 8. 14: Mô hình PC kết nối Router

3.2.Yêu cầu

- + Đặt địa chỉ ip cho từng máy PC như mô hình 8.14.
- + Cấu hình RIP để 3 router CNTT, CoKhi và DienTu thông mạng với nhau.
- + Sử dụng lệnh ping để ping từ PC1 qua PC3, PC4 qua PC6, PC2 qua PC5.

3.3.Chuẩn bị:

Bảng 8. 1:chuẩn bị phần mềm cài đặt, máy tính, router, switch thực hành bài tập 8.1

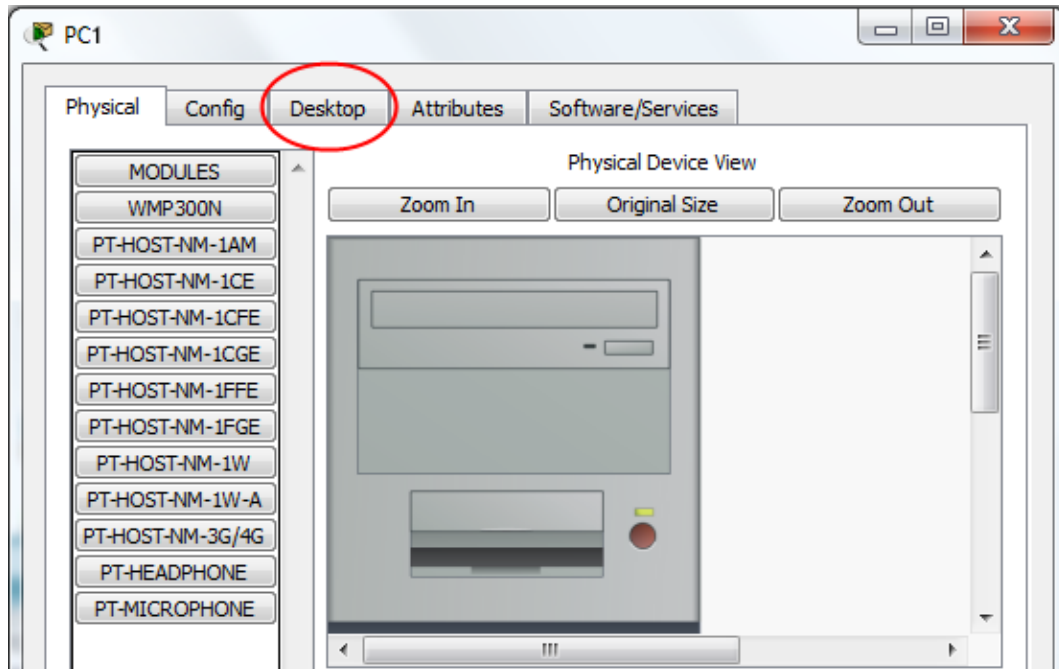
TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Phần mềm Cisco Packet Tracer	Phần mềm	1	
2	Máy PC ảo	Máy	6	
3	Router ảo	Cái	3	

4	Swicth ảo	Cái	3	
---	-----------	-----	---	--

3.4.Các bước thực hành:

Bước 1: Đặt địa chỉ IP cho PC1 :

- Nhấn vào PC1 sau đó chuyển sang tab Desktop như hình:



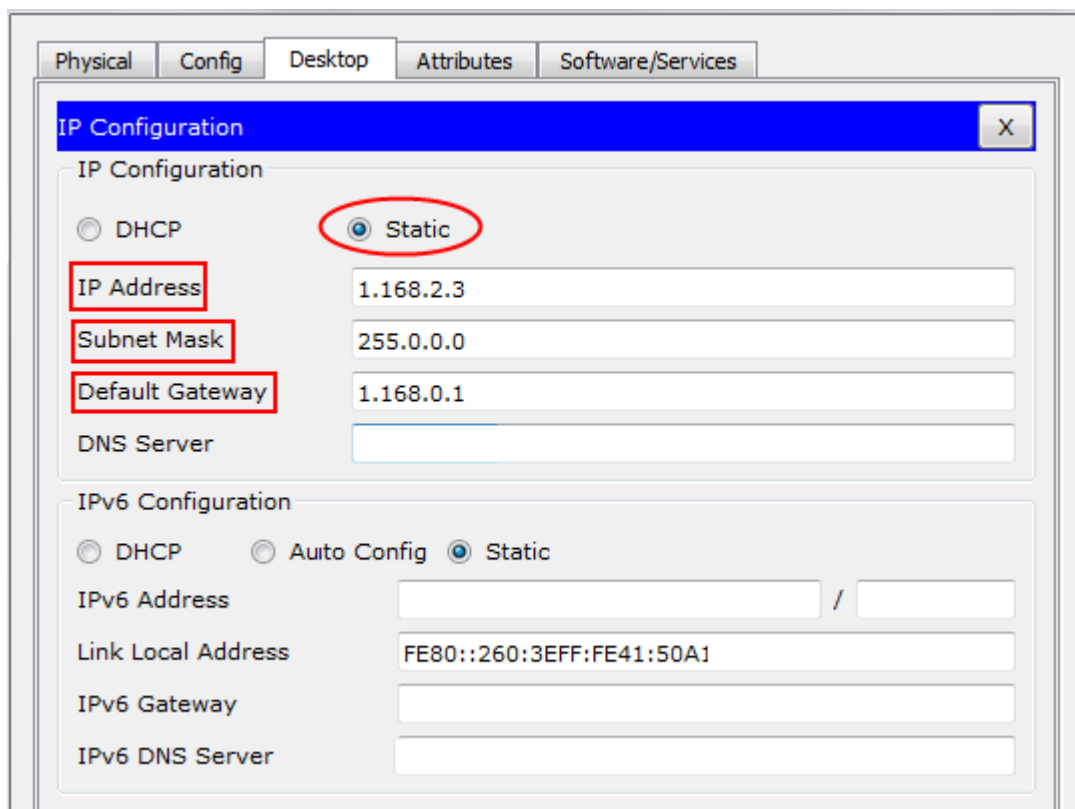
Hình 8. 15: Chuyển sang tab Desktop

- Sau đó chọn IP Configuration:



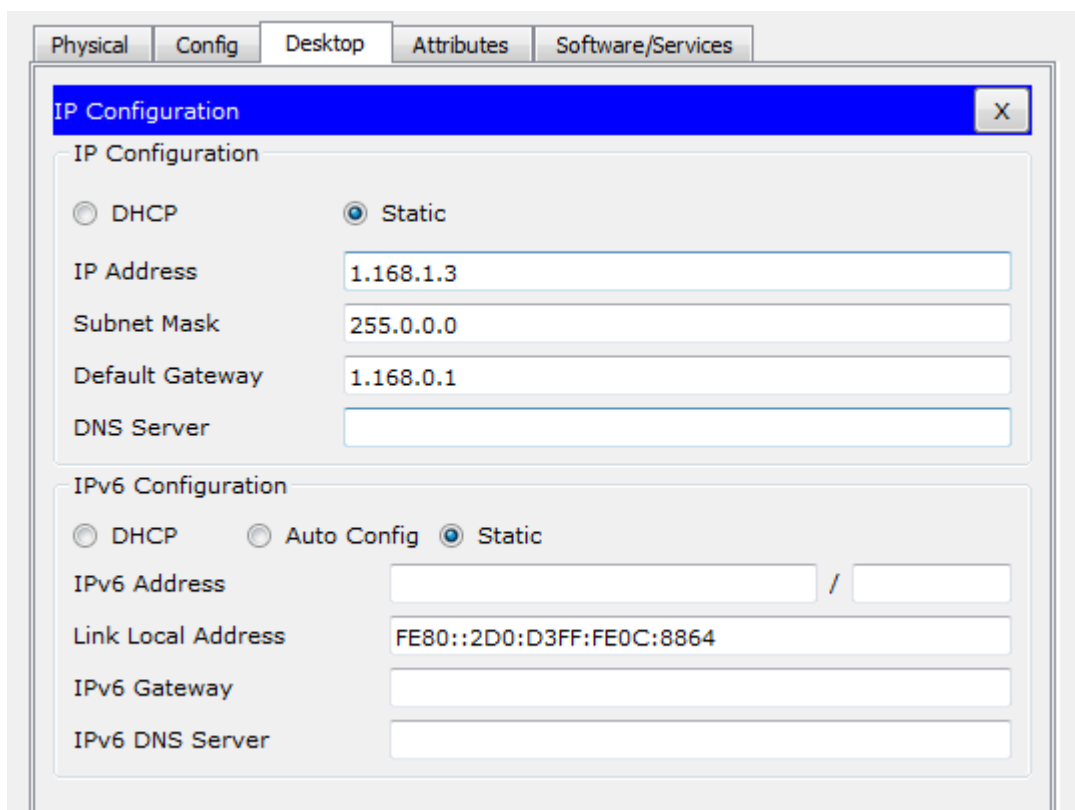
Hình 8. 16: Chọn IP Configuration

- Sau đó ta chọn Static và nhập địa chỉ IP, Subnet Mask và Default Gateway vào mục tương ứng như hình 8.17.



Hình 8. 17: Nhập các địa chỉ IP, Subnet Mask và Default GateWay cho PC1

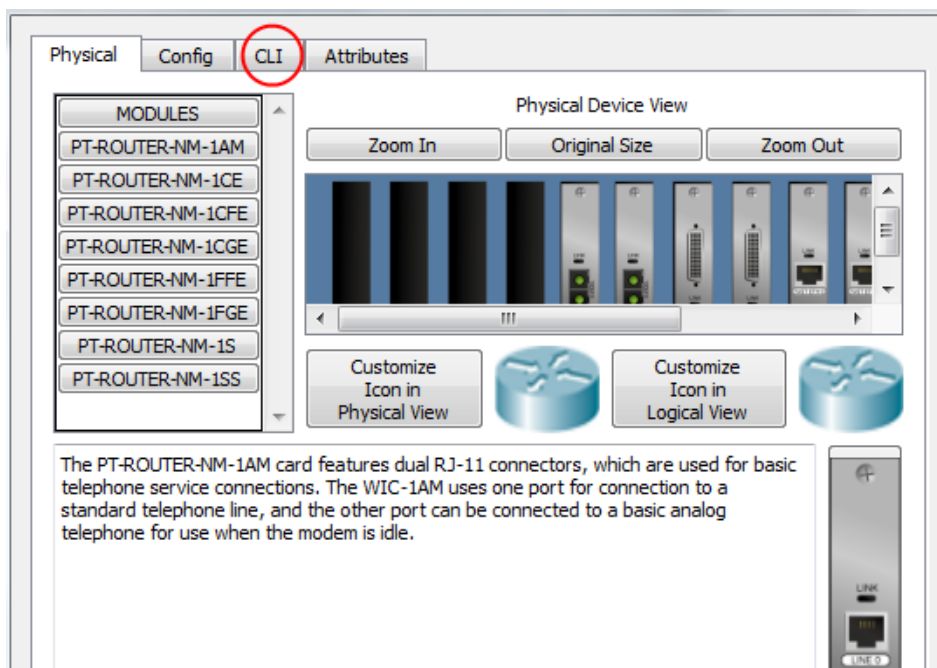
Bước 2: Tương tự với PC2 và các PC còn lại:



Hình 8. 18: Nhập các địa chỉ IP, Subnet Mask và Default GateWay cho PC2

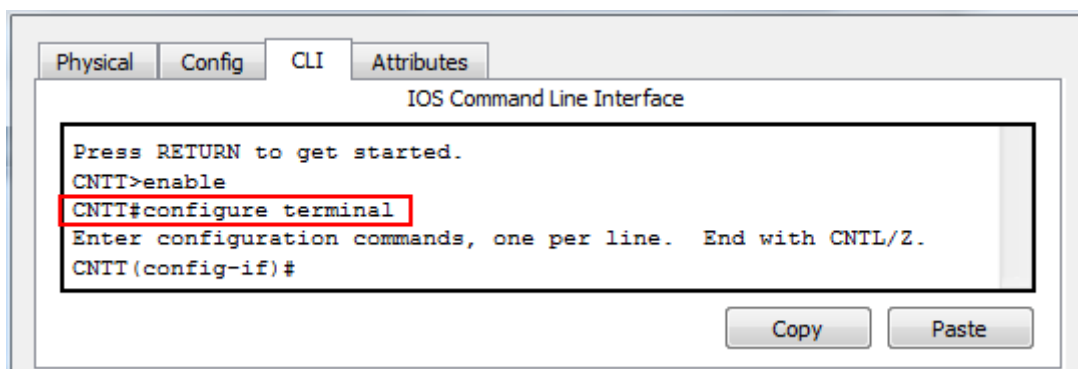
Bước 3: Cấu hình cho Router CNTT:

- Từ giao diện Physical ta chuyển sang tab CLI .



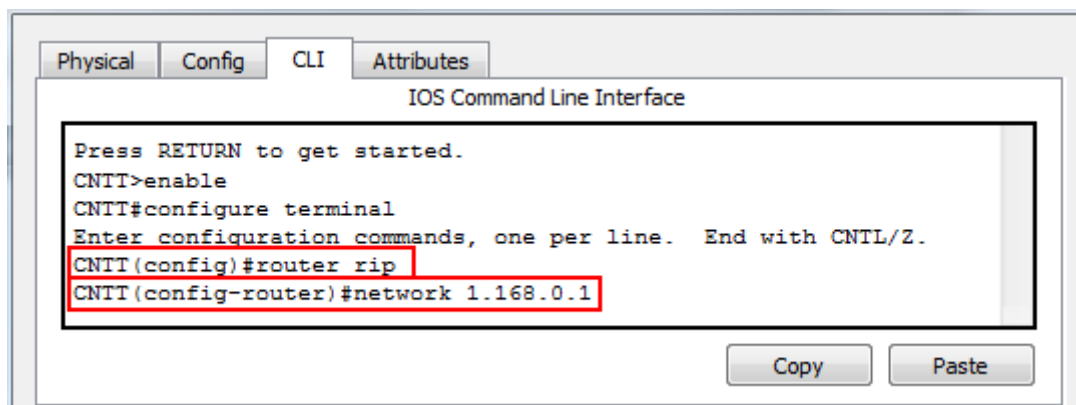
Hình 8. 19: Chuyển sang tab CLI

Bước 4: Sau đó gõ lệnh **configure terminal** để chuyển sang chế độ toàn cục.



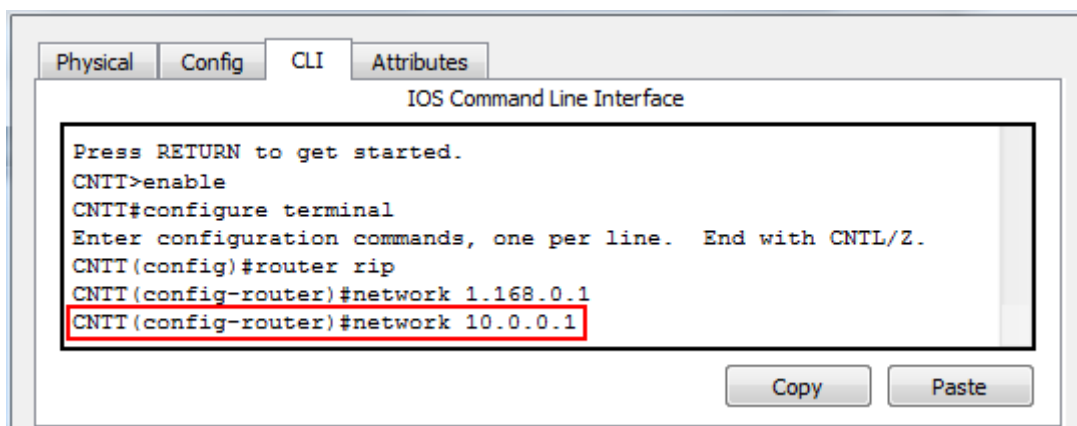
Hình 8. 20: Chuyển sang chế độ toàn cục

- Gõ tiếp lệnh **router rip** để chuyển sang chế độ cấu hình rip.
- Nhập lệnh **network** <địa chỉ ip của cổng FastEthernet 0/0> như hình 7.25.



Hình 8. 21: Cấu hình RIP cổng FastEthernet 0/0

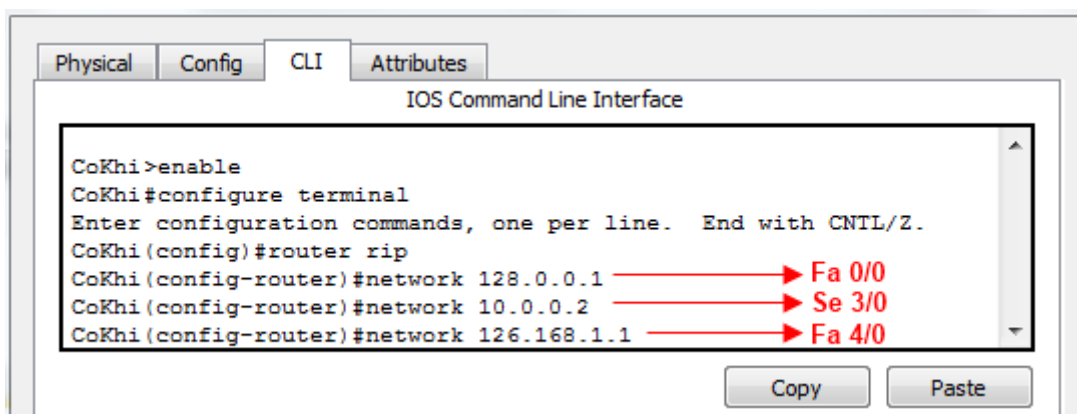
Bước 5: Nhập tiếp lệnh **network** <địa chỉ ip của cổng Serial 2/0>



Hình 8. 22: Cấu hình RIP cổng Serial 2/0

Bước 6: Vào Router CoKhi tương tự như vào Router CNTT

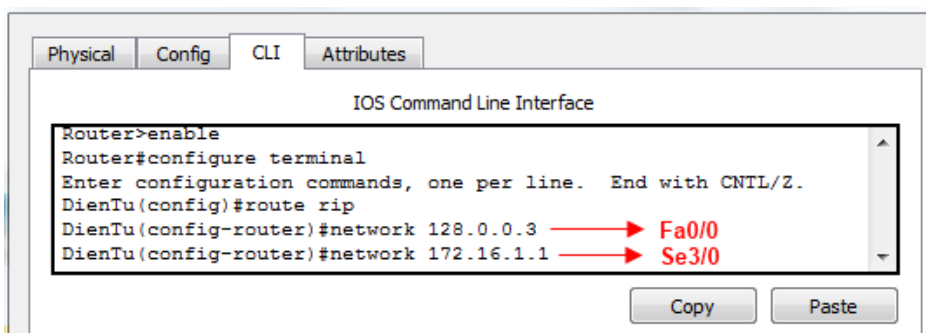
- Ta nhập lệnh Network cho các cổng Fa 0/0, Se 3/0, Fa 4/0 của RouterCoKhi



Hình 8. 23: Cấu hình RIP cho RouterCoKhi

Bước 7: Vào Router DienTu tương tự như 2 Router trước

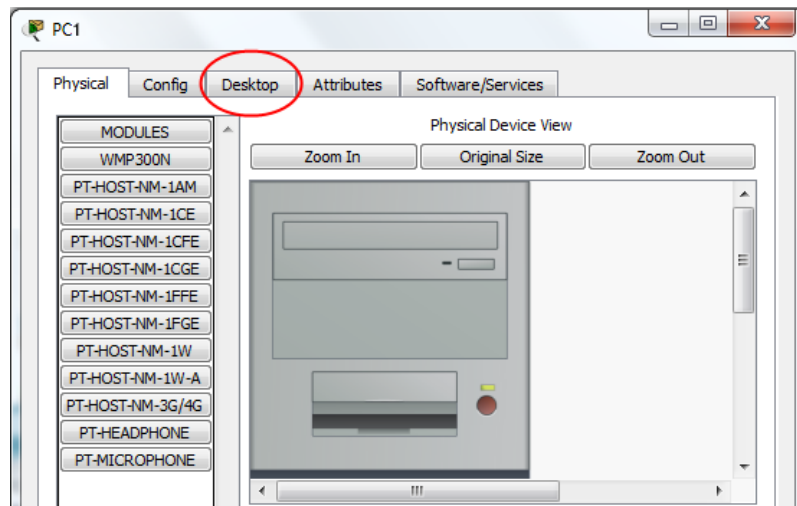
- Ta nhập lệnh Network cho các cổng Fa 0/0, Se 3/0 của RouterDienTu



Hình 8. 24: Cấu hình RIP cho RouterDienTu

Bước 8: Ping các PC1 với PC3:

- Trước tiên ta nhấn vào PC1, sau đó chuyển sang tab Desktop.



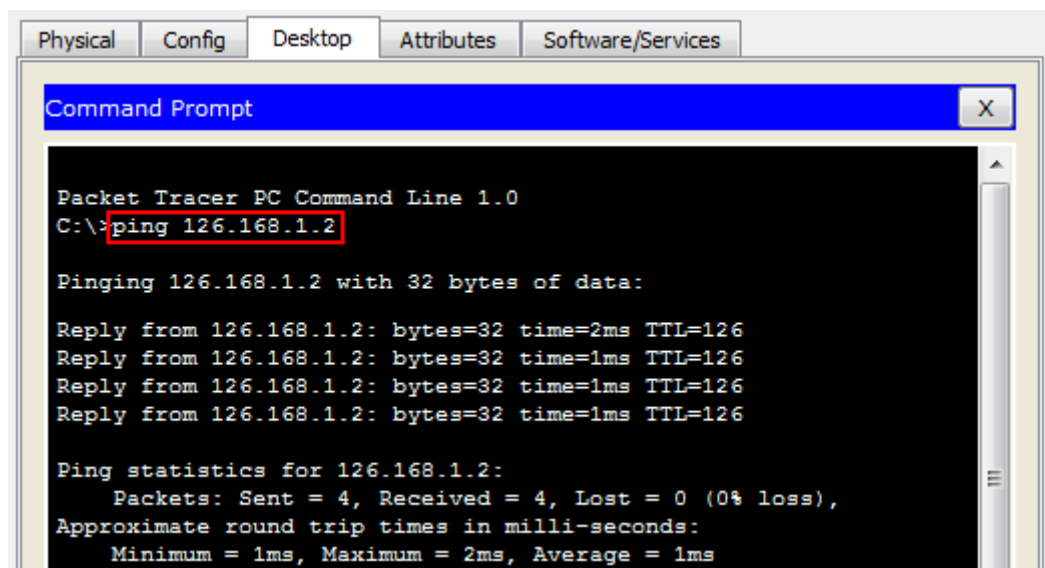
Hình 8. 25: Chuyển sang tab Desktop

- Sau đó ta chọn Command Prompt



Hình 8. 26: Chọn Cammand Prompt

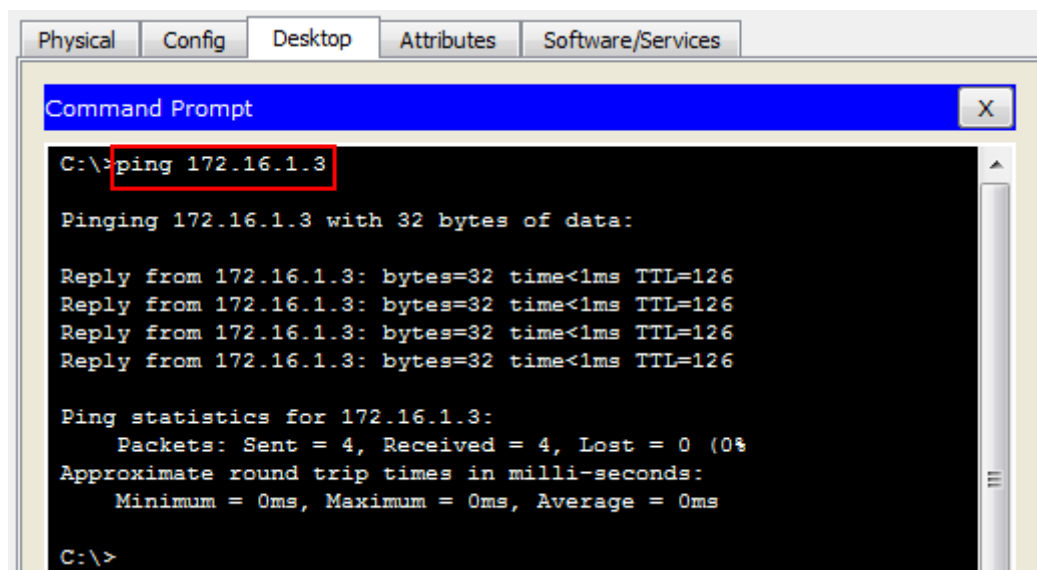
- Ta gõ lệnh Ping [địa chỉ IP đích] sau đó nhấn Enter.



Hình 8. 27: Ta gõ lệnh ping + địa chỉ ip của pc3

- Kiểm tra thấy 4 dòng *Reply from 126.168.1.2: bytes=32 time=2ms TTL=126* như hình 8.27 là ping thành công.

Bước 9: Tương tự ta ping PC4 với PC6 và các PC khác:



Hình 8. 28: Ta gõ lệnh ping +địa chỉ ip của pc6

3.5.Những sự cố thường gặp

Bảng 8. 2: những sự cố thường gặp của bài tập 8.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Không kết nối được PC với router	Chọn sai router	Chọn router CNTT và bật chế độ mở
Không nhập được địa chỉ IP	Chọn sai máy server, máy PC	Chọn lại máy server máy PC và đặt lại địa chỉ IP
Không cấu hình được chế độ toàn cục	Chưa cập nhật	Lưu và cập nhật
Không cấu hình được giao thức định tuyến	Đặt sai địa chỉ IP	Kiểm tra đặt lại địa chỉ IP và quan sát quá trình định tuyến

3.6.Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

3.7.Đánh giá các bước thực hành

Bảng 8. 3: đánh giá các bước thực hành bài tập 8.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1:Đặt địa chỉ IP cho PC1	Nhập đúng địa chỉ IP			
2	Bước 2:Tương tự với PC2 và các PC còn lại	Nhập đúng địa chỉ IP			
3	Bước 3:Cấu hình cho Router CNTT	Chọn đúng router			
4	Bước 4:Nhập lệnh configure terminal để chuyển sang chế độ toàn cục	Chọn đúng router			
5	Bước 5:Nhập tiếp lệnh network <địa chỉ ip của cổng Serial 2/0>	Nhập đúng dòng lệnh và đúng địa chỉ IP			
6	Bước 6:Vào Router DienTu tương tự như 2 Router trước	Chọn đúng router			
7	Bước 7:Ping các PC1 với PC3	Nhập đúng địa chỉ IP			
8	Bước 8:ping PC4 với PC6 và các PC khác	Nhập đúng địa chỉ IP			

4.TÓM TẮT NỘI DUNG

- IP là cơ chế tự nỗ lực tối đa để truyền gói dữ liệu. IP sử dụng thông điệp ICMP để thông báo cho máy nguồn biết là dữ liệu đã không chuyển tới được đến đích.
- Thông điệp ICMP echo request và echo reply cho phép người quản trị mạng kiểm tra kết nối IP trong quá trình xử lý sự cố mạng.
- Thông điệp ICMP cũng được vận chuyển bằng giao thức IP nên quá trình truyền thông điệp ICMP không tin cậy.
- Gói ICMP có phần Header riêng đặc biệt bắt đầu bằng phần Type và Code.
- Xác định được nguyên nhân tạo ra các thông điệp báo lỗi của ICMP.

- Chức năng của các thông điệp điều khiển ICMP.
- Thông điệp ICMP redirect/change request .
- Thông điệp ICMP để đồng bộ đồng hồ và ước lượng thời gian truyền dữ liệu.
- Thông điệp ICMP information request và reply.
- Thông điệp ICMP để tìm router .
- Thông điệp ICMP router solicitation.
- Thông điệp ICMP để báo nghẽn và điều khiển luồng dữ liệu

5.CÂU HỎI VÀ BÀI TẬP

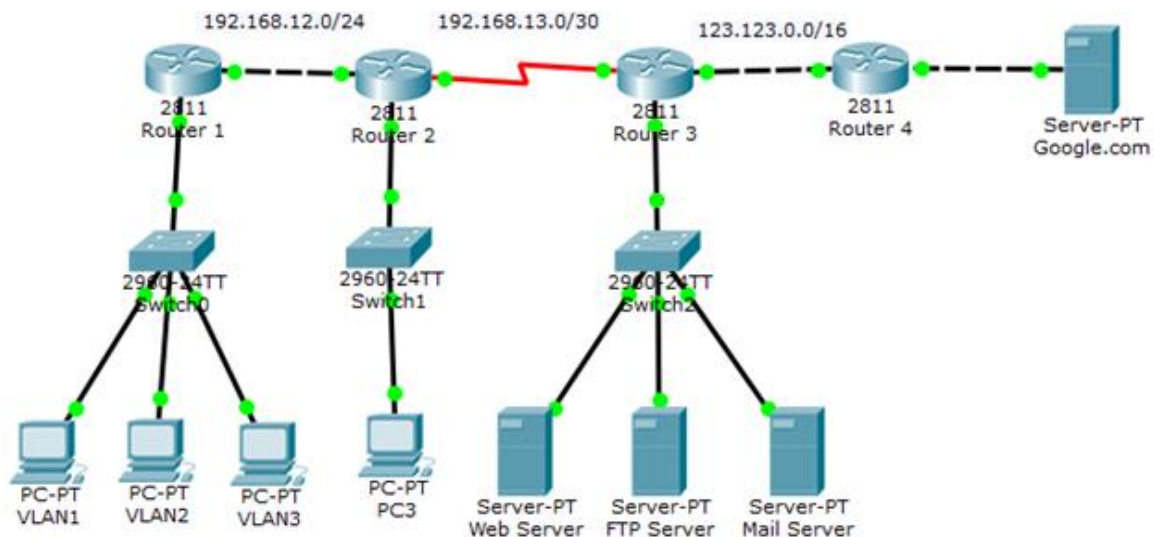
Câu hỏi:

Câu 1: Trình bày giao thức thông điệp điều khiển Internet (IMCP)?

Câu 2: Trình bày đồng bộ đồng hồ và ước tính Thời gian truyền dữ liệu?

Bài tập:

Cho mô hình mạng như hình :



- Đặt IP theo sơ đồ. Mô tả các interface đầu nối.
- Cấu hình Access List cho Router.
- Kết hợp cấu hình định tuyến động RIPv2 và cấu hình tính năng DHCP relay trên Router Cisco.

BÀI 9 : CAMERA

Mã bài MD 28-09

Thời gian: 15 giờ

I.MỤC TIÊU: Sau khi học xong bài này, sinh viên có các khả năng sau:

- Phân loại và xác định được công nghệ camera
- Trình bày được quy trình cài đặt, cấu hình camera
- Thực hành đúng quy trình cài đặt, cấu hình camera
- Kiểm tra được quy trình đã cài đặt, cấu hình camera
- Thực hiện thao tác an toàn trên máy tính và hệ thống camera
- Rèn luyện được tính cẩn thận, chính xác, làm việc theo đúng quy trình

II.NỘI DUNG CHÍNH

1.Giới thiệu về camera

Camera quan sát là việc sử dụng các mắt điện tử để ghi lại những hình ảnh, video lại vị trí lắp các mắt điện tử, những hình ảnh đó sẽ được lưu lại và phát trực tiếp lên màn hình cho chúng ta giám sát, quản lý hay xử lý những sự cố không đáng có xảy ra.

2.Phân loại về camera

2.1 Phân loại

Camera ngoài trời : là camera thiết kế dạng thân trụ, có kèm chân đế. Loại **camera quan sát** này được thiết kế để lắp đặt ngoài trời, đã được tích hợp chuẩn chống thấm nước, bụi bẩn IP66 và chống va đập IK10. Camera quan sát ngoài trời có hồng ngoại tự động chuyển ngày đêm giúp quan sát liên tục và cho hình ảnh sắc nét hơn.

Camera trong nhà : là camera thiết kế dạng bán cầu (dome), thiết kế nhỏ gọn, đẹp mắt để lắp đặt trong nhà không làm mất mỹ quan và vì không tích hợp chuẩn IP66 nên không chống chịu được mưa nắng. Loại camera quan sát này khi lắp đặt chú ý không lắp những vị trí ẩm thấp, camera có hồng ngoại chuyển ngày đêm cho hình ảnh đẹp và quan sát liên tục ban ngày lẫn ban đêm.



Hình 9. 1: các loại camera

2.2 Công nghệ camera

Công nghệ IP: Công nghệ thứ 3 được phát triển đó chính là công nghệ IP, là loại camera quan sát có hình ảnh được số hóa, xử lý và mã hóa từ bên trong, sau đó truyền tải tín hiệu ảnh số qua một kết nối Ethernet về máy vi tính, cũng có thể là một thiết bị lưu trữ tín hiệu số như: Hệ thống NAS, hệ thống server hoặc đầu ghi hình IP....Camera IP có thể sử dụng 2 loại cảm biến CMOS hoặc CCD, và cũng có nhiều hình dáng tương tự như các dòng camera Analog truyền thống như Pan/Tilt/Zoom, mái vòm, đầu đạn, ngụy trang, hộp, hồng ngoại và không dây....Camera IP thông thường được tích hợp sẵn một giao diện web để có thể truy cập và quản lý dựa trên 1 địa chỉ IP xác định thông qua mạng WAN, LAN hoặc Internet. Do vậy bạn hoàn toàn có thể xem camera mà không cần đầu thu hình

Công nghệ HD AHD: AHD là viết tắt của (Analog High Definition) công nghệ camera analog đạt đến chất lượng HD. Do đó, tín hiệu hình ảnh truyền đi mà không cần phải nén lại như HDCVI là HD-SDI. Tín hiệu truyền dẫn trên cáp đồng trục có thể lên đến 500m.

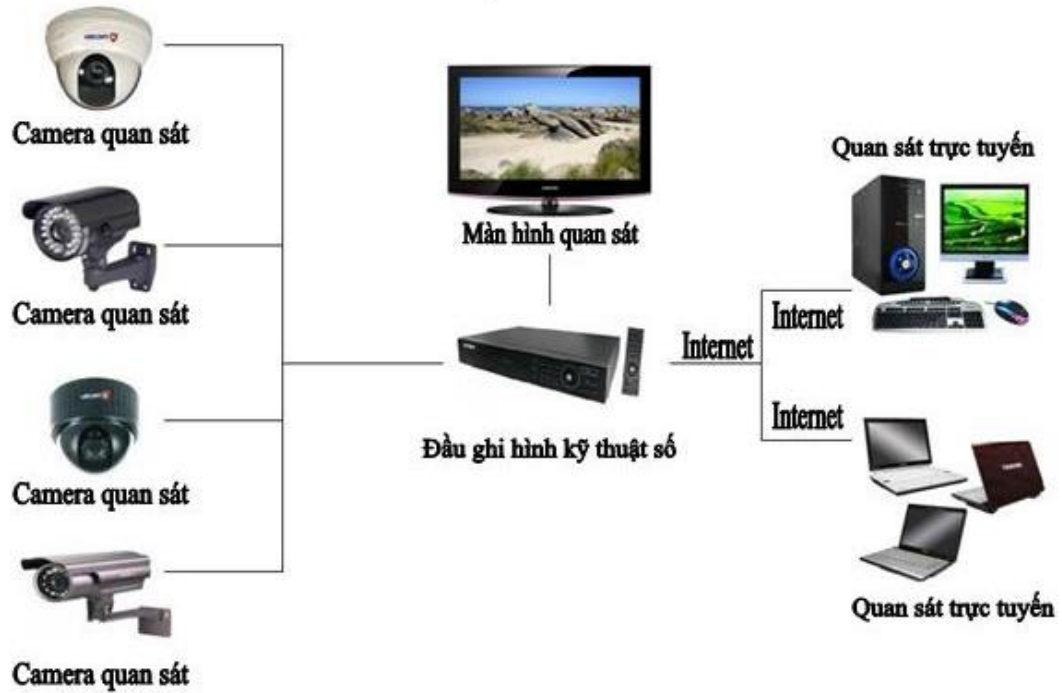
Công nghệ HD CVI: HD CVI (Công nghệ truyền tải hình ảnh độ phân giải cao) là công nghệ truyền tín hiệu hình ảnh chất lượng cao HD thông qua dây cáp đồng trục. HDCVI cung cấp 2 định dạng video chuẩn HD là 1280H (độ phân giải 1280x720) và 1920H (độ phân giải 1920x1080). Cho chất lượng hình ảnh cao hơn rất nhiều so với các định dạng video độ nét tiêu chuẩn như độ phân giải D1 720H (720x576) và độ phân giải 960H (960x576).

Công nghệ HD TVI: Công nghệ HDTVI (hay còn được gọi là HD-TVI - High Definition Transport Video Interface) có nghĩa là giao thức truyền tải hình ảnh độ nét cao. Đây là công nghệ DSP-TVI, được phát triển bởi công ty Techpoint (năm 2012), và phần chip xử lý được bán cho công ty Intersil tiếp tục nghiên cứu và phát triển. Giải pháp HD-TVI, giải quyết được những vấn đề trước đây của công nghệ HD-SDI và HDCVI. Công nghệ HDTVI có thể chuyển đổi các tín hiệu kỹ thuật số thành tín hiệu analog tương tự, công nghệ này còn mở rộng khoảng cách truyền tải, giảm tổng chi phí sản phẩm, và chiếm ít dung lượng lưu trữ hơn.

3. Bài tập 9.1, thực hành cài đặt, cấu hình camera IP có dây

3.1 Sơ đồ hệ thống camera

SƠ ĐỒ KẾT NỐI HỆ THỐNG CAMERA CÓ DÂY



Hình 9. 2: hệ thống camera IP sử dụng dây cáp mạng

3.2.Yêu cầu

Thực hiện lắp đặt hệ thống camera theo sơ đồ, cài đặt, cấu hình để hệ thống vận hành tốt

3.3.Chuẩn bị:

Bảng 9. 1: chuẩn bị thiết bị, vật tư thực hành bài tập 9.1

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Đầu ghi hình Camera	Cái	4	
2	Đầu thu hình	Cái	1	
3	Màn hình TV	Cái	1	
4	Swicth	Cái	1	
5	Dây nguồn 12V	Sợi	2	
6	Dây cáp tín hiệu	Sợi	2	
7	Cáp HDMI (hoặc cáp VGA)	Sợi	2	
8	Tắc kê & ốc vít	Con	20	
9	Các đầu Jack kết nối: Jack BNC và Jack RJ45	Đầu	10	
10	Đường truyền internet	Đườn truyền	1	

3.4.Các bước thực hành

Lắp đặt camera vào đúng các vị trí cần quan sát

Cách chọn vị trí lắp đặt camera: Ngoài chất lượng camera thì việc chọn đúng vị trí lắp camera có ý nghĩa khá quan trọng:

- Vị trí cần bao quát: vị trí đặt camera cần có góc quan sát rộng, cao và thông thoáng, không bị khuất tầm nhìn. Độ cao nên từ 2,5m – 3,5m là vừa chừng.
- Bán kính quan sát: với các camera phân khúc tầm trung thì khoảng tối đa từ camera đến đối tượng cần quan sát nên ở khoảng 10m trở lại, nhằm giúp việc quan sát và truy xuất lại hình ảnh được rõ nét hơn. Đặc biệt lưu ý đến tầm xa hồng ngoại để chọn khoảng cách quan sát khi trời tối.
- Tránh ngược sáng: dù camera bạn có độ nét cỡ nào thì khi quan sát ngược sáng hình ảnh luôn bị tối, mờ và không rõ nét. Tốt nhất bạn nên hạn chế tối đa việc hướng quan sát của camera bị ngược nắng. Tránh đặt camera trong góc quá tối nhìn ra ánh sáng quá mạnh và ngược lại (một số trường hợp đèn hồng ngoại sẽ bật lên vì nhầm tưởng là ban đêm).
- Tránh tiếp xúc trực tiếp với ánh nắng gắt hoặc nước mưa (dù bạn đang chọn loại camera ngoài trời với tiêu chuẩn chống bụi & nước IP67). Nên chọn lắp dưới các góc có mái che. Hoặc nếu phải lắp trực tiếp ngoài trời thì bạn nên chọn mua hộp che camera ngoài trời để bảo quản camera được tốt hơn.

Lắp và cố định vị trí camera

Đầu tiên, các bạn sẽ tiến hành tháo rời các bộ phận bên trong camera trước khi tiến hành lắp đặt lên trần nhà hoặc lên tường nhà.

Để làm điều này, các bạn cần hiểu qua kết cấu một số loại camera thông dụng để biết cách tháo & lắp camera.

Có 02 loại camera cơ bản:

- + Camera dome: còn gọi là camera dạng cầu, thường dùng để lắp camera trong nhà.
- + Camera bullet: còn gọi là camera dạng thân, thường dùng để lắp camera ngoài trời.

Lắp đặt đầu ghi cố định

Chọn vị trí hợp lý để lắp đầu ghi

- Quan trọng chúng ta nên chọn vị trí lắp đầu ghi ở những nơi thoáng mát (tránh quá nhiệt) và an toàn, tránh bị người khác lấy mất. Ngoài ra nên chọn vị trí đầu ghi đặt gần khu vực gần màn hình LCD quan sát (nếu có) để dễ đi dây HDMI nối từ đầu ghi về màn hình LCD theo dõi. Độ dài dây HDMI thông dụng trên thị trường khoảng 2,5m.

LƯU Ý KHI THỰC HÀNH:

- + Kiểm tra và cố định các bó dây cáp, cho vào nẹp điện hoặc cố định chắc chắn bằng dây gút (lạc nhựa) thật kỹ càng.
- + Đậy tất cả các nắp dây mà ta mở ra lúc thi công như: nắp trần thạch cao, hộp điện, hộp nguồn kỹ thuật camera (hộp liên nguồn)
- + Cố định lại nẹp điện hoặc các bộ phận còn lỏng lẻo.
- + Kiểm tra và quấn băng keo các phần dây tiếp xúc ngoài trời. Đảm bảo nước mưa không thấm vào các mối nối dây cáp tín hiệu hoặc dây nguồn...
- + Kiểm tra tính thẩm mỹ của toàn bộ công trình lần cuối.
- + Thu gom rác, vệ sinh và dọn dẹp đồ nghề.

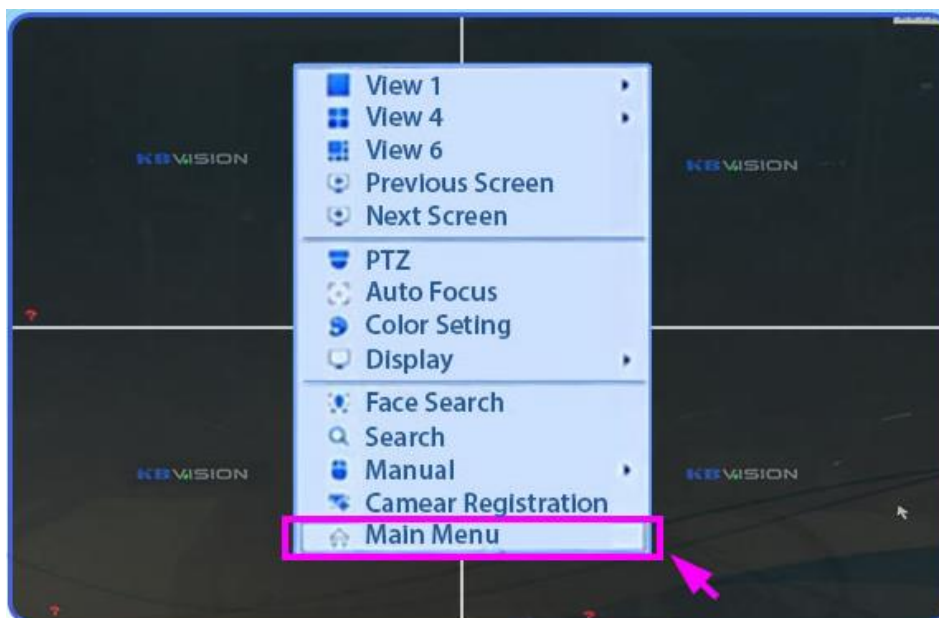
Cài đặt đầu ghi để xem camera qua internet (không cần tên miền)

- Các loại đầu ghi đời mới khoảng vài năm gần đây đều có hỗ trợ công nghệ P2P (point to point). Với công nghệ này chúng ta có thể thiết lập cho đầu ghi kết nối internet mà không cần nhiều công đoạn phức tạp như mở port cho modem, cấu hình tên miền động...

Các bước cài đặt đầu trên đầu ghi: đảm bảo đã kết nối cáp mạng từ đầu ghi đến modem (thông qua 2 đầu Jack RJ45). Dùng chuột để tiến hành các bước cài đặt trên đầu ghi như sau:

Bước 1: Vào phần main menu trên đầu ghi

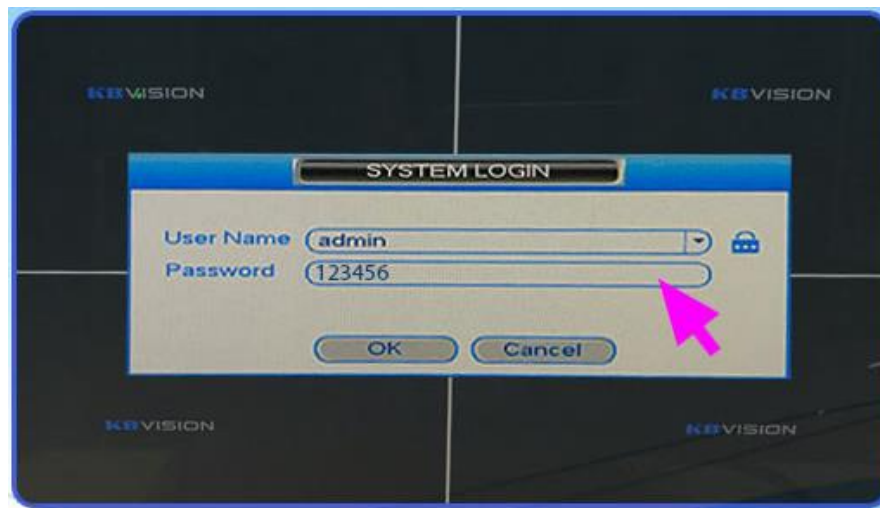
Tại màn hình đầu ghi (hiển thị trên Tivi LCD), bạn click chuột phải vào giữa màn hình. Sau đó chọn mục “**Main Menu**”



Hình 9. 3: màn hình chính của main menu

Bước 2: Thông tin đăng nhập đầu ghi

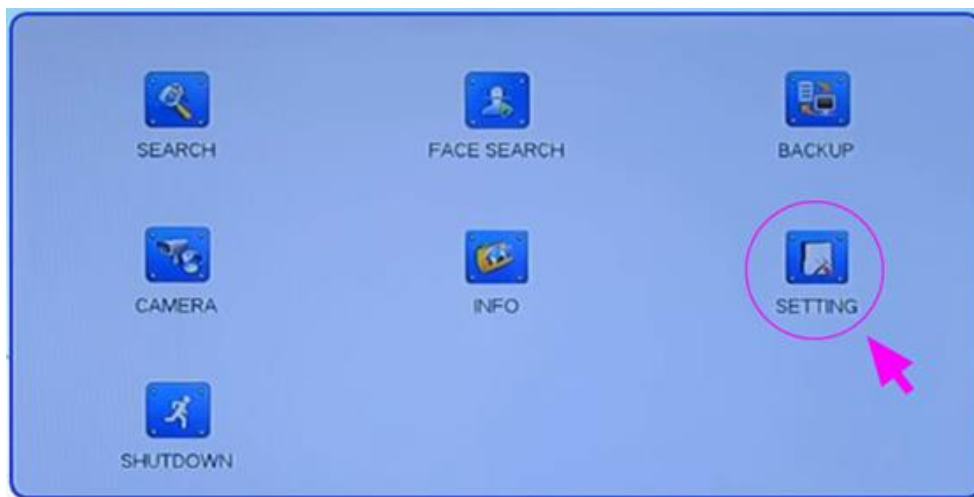
Nhập username: **admin**; và password mặc định là: **123456**, sau đó chọn OK.



Hình 9. 4: giao diện nhập thông tin

Bước 3: Cài đặt

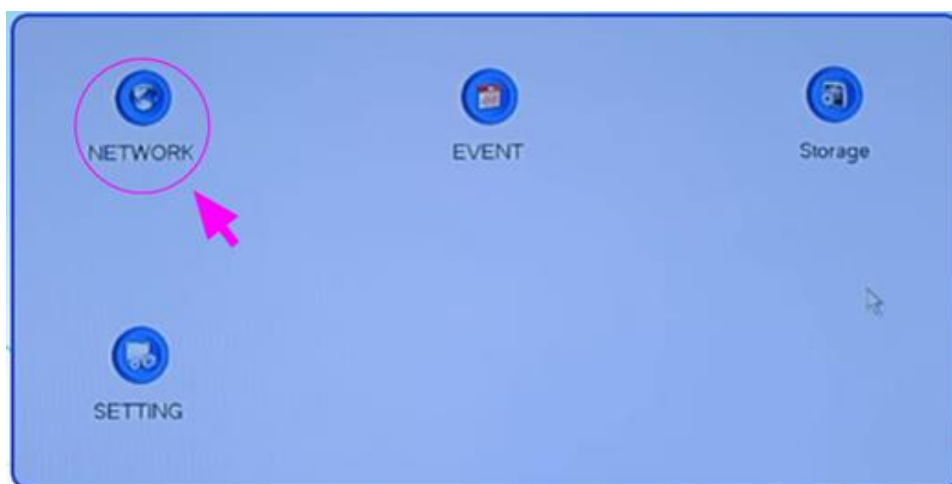
Tại màn hình tiếp theo, chọn mục “Setting”



Hình 9. 5: giao diện màn hình nền

Bước 4: Cài đặt Network

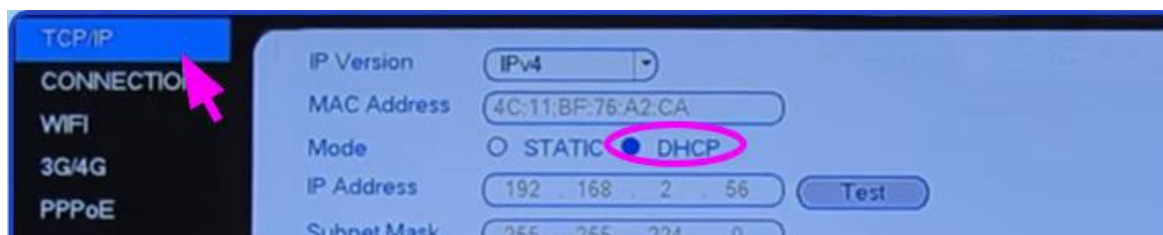
Chọn tiếp mục “Network”



Hình 9. 6: : Cách set up đầu ghi xem camera từ xa

Bước 5: Bật DHCP

Đảm bảo mục DHCP đã được bật (dấu tick màu xanh).



Hình 9. 7: : bật chế độ DHCP

Bước 6: Cấu hình P2P (xem camera không cần tên miền DNS)

Chọn tiếp mục “P2P”, kích hoạt lựa chọn “Enable P2P”.

Một màn hình QR Code sẽ hiện lên như sau:



Hình 9. 8: chế độ xem camera

3.5.Những sự cố thường gặp

Bảng 9. 2:những sự cố thường gặp của bài tập 9.1

Hiện tượng	Nguyên nhân	Hướng khắc phục
Khởi động máy tính không nhận camera	Khai báo sai thông số	Đọc kỹ thông số của nhà sản xuất cung cấp và khai báo lại
Đặt địa chỉ IP không được	Do trùng địa chỉ IP	Dùng lệnh Ipconfig kiểm tra và đặt lại địa chỉ IP
Không cài đặt được dịch vụ DHCP	Chưa bật chế độ mở cho dịch vụ DHCP	Kiểm tra check lại chế
Hình ảnh bị nhòe khi xem trên tivi	Do setup chế độ xem không đúng với dung lượng của card màn hình	Setup lại chế độ xem hình ảnh

3.6. Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

.....

.....

.....

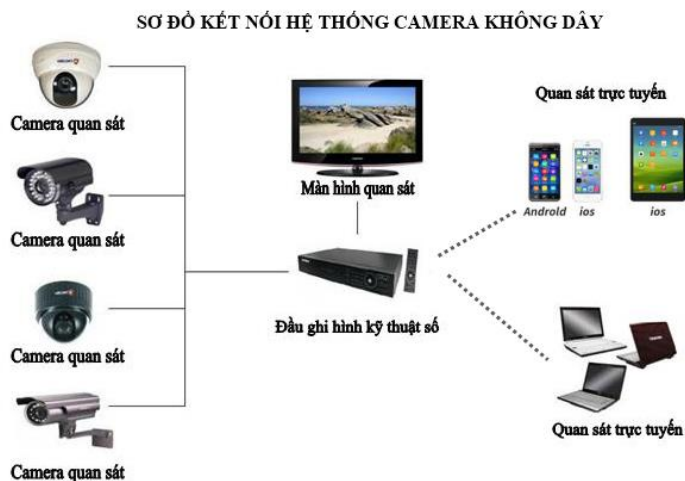
3.7. Đánh giá các bước thực hành

Bảng 9. 3: đánh giá các bước thực hành bài tập 9.1

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1: Vào phần main menu trên đầu ghi khai báo thông số	Khai báo đúng các thông số			
2	Bước 2: Thông tin đăng nhập đầu ghi	Nhập thông tin của người quản lý			
3	Bước 3: Cài đặt camera	Chọn đúng các mục			
4	Bước 4: Cài đặt Network	Chọn đúng IP			
5	Bước 5: Bật DHCP	Chọn đúng chế độ			
6	Bước 6: Cấu hình P2P (xem camera không cần tên miền DNS)	Chọn đúng các mục			

4. Bài tập 9.2, thực hành cài đặt, cấu hình camera IP không dây

4.1. Sơ đồ hệ thống camera



Hình 9. 9: hệ thống camera sử dụng wifi

4.2.Yêu cầu

Lắp đặt hệ thống camera, cài đặt, cấu hình hệ thống camera sử dụng wifi

4.3.Chuẩn bị:

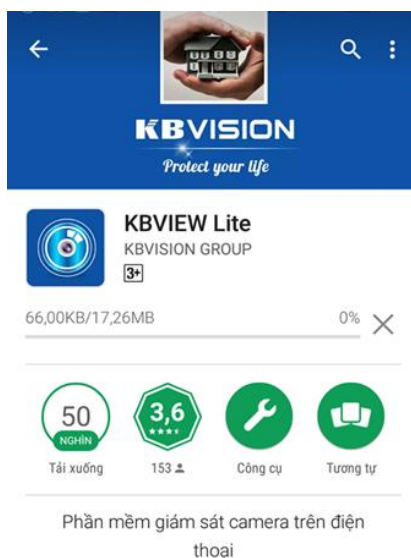
Bảng 9. 4: chuẩn bị thiết bị thực hành bài tập 9.2

TT	Máy tính, thiết bị, phần mềm	Đơn vị	Số lượng	Ghi chú
1	Đầu ghi hình Camera	Cái	1	
2	Điện thoại smart phone	Cái	1	
3	Laptop	Cái	1	
4	Đường truyền internet	Đườn truyền	1	

4.4.Các bước thực hành

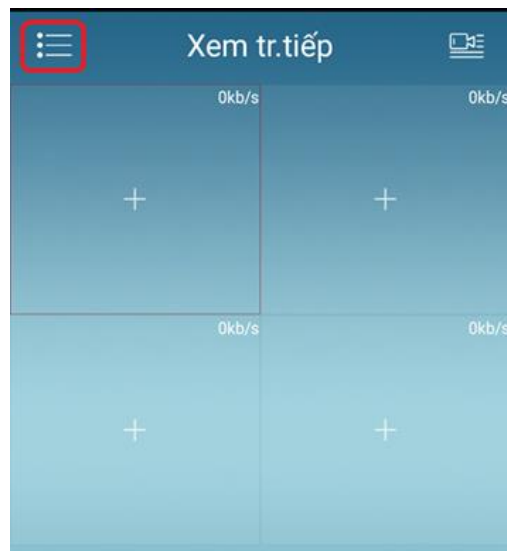
4.4.1.Cài đặt và cấu hình Camera trên điện thoại Smart phone:

Bước 1: Đối với điện thoại thì ta cần tải ứng dụng KBVIEW Lite về máy, hệ điều hành Android chúng ta vào CH Play để tải còn IOS thì vào App Store để tải về. Sau đó chúng ta mở phần mềm KBVIEW Lite lên.



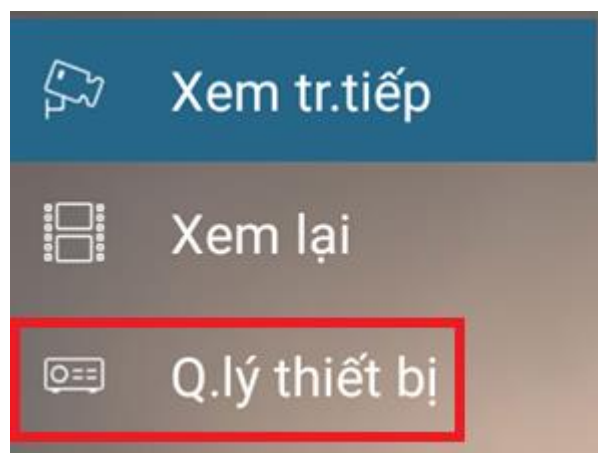
Hình 9. 10: giao diện giám sát camera

Bước 2: Chúng ta chọn phần 3 gạch ngang phía bên trái trên cùng của ứng dụng **KBVIEW Lite**.



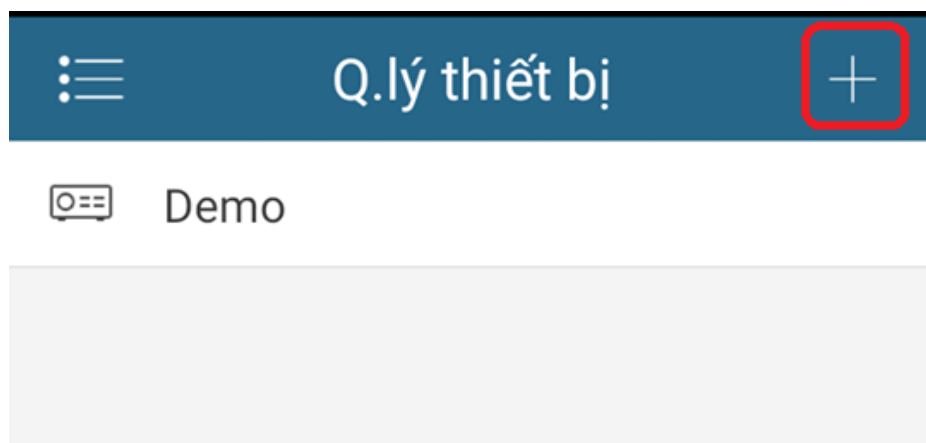
Hình 9. 11: màn hình camera xem trực tiếp

Bước 3: Chọn phần quản lý thiết bị để vào phần cài đặt xem camera cho điện thoại.



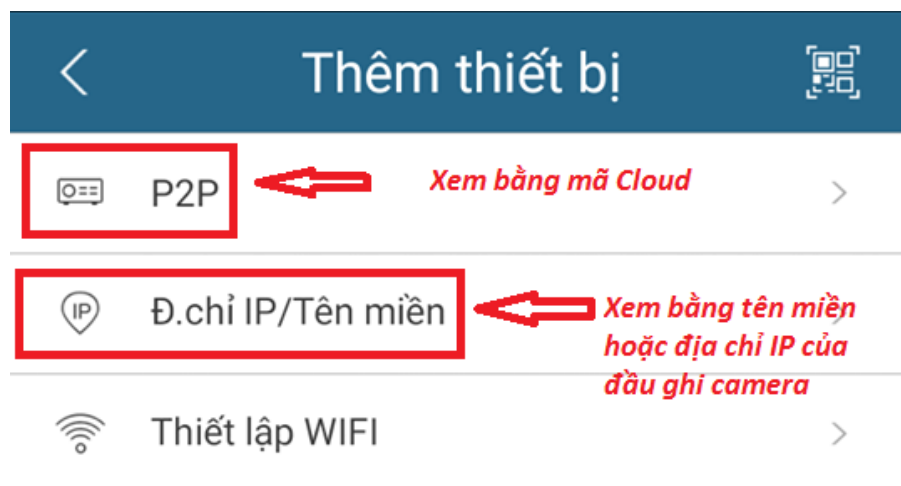
Hình 9. 12: : màn hình quản lý thiết bị

Bước 4: Chọn mục dấu "+" để cài đặt.



Hình 9. 13: màn hình cài đặt quản lý thiết bị

Bước 5: Trong phần này có 2 loại cho chúng ta cài đặt.



Hình 9. 14: menu thêm thiết bị

- Cài đặt xem camera Kbvision bằng Cloud: Nếu khách hàng muốn xem camera Kbvision bằng mã Cloud thì chọn vào mục P2P sau đó cài đặt như sau:
 - + Tên: Phần này khách hàng đặt tùy thích theo ý của mình.
 - + SN: phần này khách hàng nhập mã Cloud của mình vào.
 - + Tên đăng nhập: admin
 - + Mật khẩu: nhập mật khẩu do bên camera cung cấp hoặc mật khẩu mà bên khách hàng đã đổi.
 - + Xem trực tiếp và xem lại có thể chọn **Chính** để lúc xem camera ở chế độ HD, nếu HD sẽ chạy chậm hơn do chiếm băng thông mạng lớn hơn.
 - + Sau đó chọn "Bắt đầu xem trực tiếp"

Hình 9. 15: các chế độ xem hình ảnh

- Cài đặt xem camera Kbvvision cho điện thoại bằng tên miền: Ta chọn phần "Địa chỉ IP/tên miền".
- + Tên: Cũng đặt theo ý thích của khách hàng để dễ phân biệt nếu có lắp đặt nhiều nơi.
- + Địa chỉ: Nhập tên miền xem camera từ xa của mình đã đăng ký, hoặc nhập địa chỉ IP của đầu ghi hình.
- + Cổng: Nhập cổng của đầu ghi hình do bên lắp camera giám sát cung cấp cho khách hàng
- + Tên đăng nhập: admin
- + Mật khẩu: nhập mật khẩu do bên camera cung cấp hoặc mật khẩu mà bên khách hàng đã đổi.
- + Xem trực tiếp và xem lại có thể chọn **Chính** để lúc xem camera ở chế độ HD, nếu HD sẽ chạy chậm hơn do chiếm băng thông mạng lớn hơn.
- + Sau đó cũng chọn mục "Bắt đầu xem trực tiếp" để hoàn tất việc cài đặt.

The screenshot shows a mobile application interface for configuring a camera. At the top, there is a blue header bar with a back arrow, the text "Đ. chỉ IP/Tên miền", and a save icon. Below the header, there are several input fields and buttons:

- A label "Chế độ đăng ký:" followed by the text "Đ. chỉ IP/Tên miền".
- A text input field labeled "Tên:" containing the value "AnThanhPhat".
- A text input field labeled "Địa chỉ:" with a red placeholder text "Nhập tên miền hoặc địa chỉ đầu ghi".
- A text input field labeled "Cổng:" containing the value "37777".
- A text input field labeled "Tên đ. nhập:" containing the value "admin".
- A text input field labeled "Mật khẩu:" with masked characters "•••••".
- A button labeled "Xem tr. tiếp:" with the text "Phụ >" next to it.
- A button labeled "Xem lại:" with the text "Phụ >" next to it.
- A large blue button at the bottom labeled "Bắt đầu xem tr. tiếp", which is highlighted with a red rectangle.

Hình 9. 16: : cài đặt chế độ xem hình ảnh có DNS

- Nếu phần mềm không tự động lưu cài đặt của mình thì khách hàng có thể lưu lại bằng cách chọn hình phía trên bên phải màn hình của ứng dụng.

4.4.2. Cài đặt xem camera Kbvvision cho máy tính.

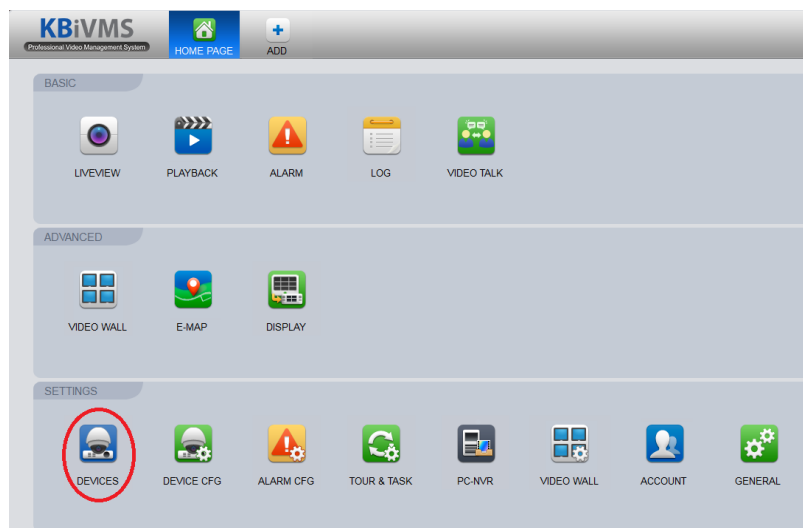
Bước 1: Để cài đặt thì chúng ta cần tải về và cài đặt phần mềm KBiVMS dành cho máy tính.

- Sau đó chúng ta mở phần mềm đã cài đặt trên máy tính, sau đó nhập Password là **admin** rồi chọn login để đăng nhập vào phần mềm.



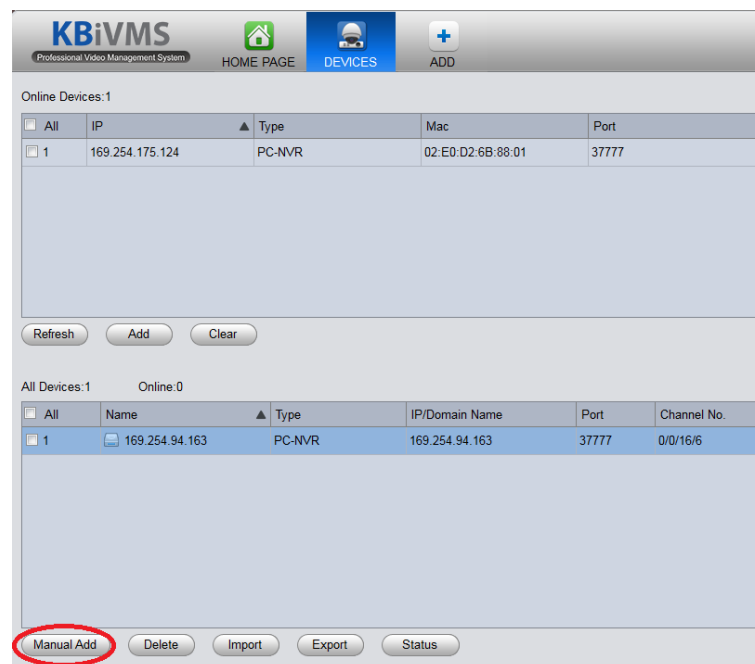
Hình 9. 17: màn hình đăng nhập

Bước 2: Tiếp theo ta chọn DEVICES để vào phần cài đặt xem camera.



Hình 9. 18: giao diện vào màn hình chính

Bước 3: Giao diện sẽ xuất hiện như hình bên dưới, chúng ta chọn vào **Manual Add** để cài đặt các phần xem camera.



Hình 9. 19: giao diện cài đặt màn hình xem camera

Bước 4: Bước này dùng để cài đặt các mục xem camera cho máy tính.

- Cài đặt xem bằng mã Cloud: Giao diện ứng dụng sẽ như hình bên dưới.
- + **Device Name:** Đặt tên tùy thích để phân biệt với các mục khác.
- + **Register Mode:** Phần này chúng ta chọn SN như hình dưới.
- + **SN:** Nhập mã Cloud xem camera của mình vào mục này.
- + **User Name:** admin
- + **Password:** Nếu đặt mật khẩu thì nhập vào, không thì để trống.

Sau đó chọn **Save and Continue** để lưu lại, như vậy là có thể xem camera bằng mã Cloud của mình.

Hình 9. 20: xem camera bằng mã Cloud

- Cài đặt xem camera kbvision bằng tên miền: Giao diện nó cũng tương tự như trên.
- + **Device Name:** Đặt tên tùy thích để nhớ để phân biệt với xem mã Cloud.
- + **Register Mode:** Chọn IP/Domain như hình bên dưới.

- + **IP/Domain Name:** Phần này khách hàng nhập tên miền đã đăng kí từ trước (Có thể xem được cả nội mạng và ngoại mạng) hoặc nhập địa chỉ IP của đầu ghi hình camera (phần này chỉ xem được nội mạng).
- + **User Name:** admin
- + **Password:** Nếu đặt thì nhập còn không để trống (Camera An Thành Phát khuyến khích khách hàng khi dùng camera bất kì hãng nào, mật khẩu nên đặt để đảm bảo tính bảo mật cao hơn, tránh bị người khác xem camera của mình làm mất đi sự riêng tư của khách hàng).

Sau đó chọn "**Save and Continue**" để lưu lại và xem camera của mình.

Hình 9. 21: Save and Continue

4.5.Những sự cố thường gặp.

Bảng 9. 5:những sự cố thường gặp của bài tập 9.2

Hiện tượng	Nguyên nhân	Hướng khắc phục
Lỗi camera không lên hình khi cắm nguồn đầu ghi	Nguồn đầu ghi hình camera bị hỏng hoặc có dấu hiện đứt Giắc nối bị hỏng hoặc chưa kết nối chặt với ổ. Đầu ghi hình bị hỏng main chip xử lý Chân cắm camera vào	Lỗi Camera không lên hình là lỗi hay xảy ra nhất trong quá trình sử dụng. Lỗi không lên hình có thể do nhiều nguyên nhân như: Đứt dây, Jack cắm bị hỏng, nguồn camera chưa có

	bom mạch bị lỗi	điện,... Vì vậy khi phát hiện ra camera bị lỗi này thì nên kiểm tra: Kiểm tra xem đường dây truyền tín hiệu có bị đứt không? Kiểm tra Jack cắm có bị lỏng hoặc bị tháo rời ra không? Camera đã báo có điện chưa? Kiểm tra nguồn điện của camera đã được cắm chưa? Đổi vị trí cắm đầu ghi hình camera sang kênh hiển thị khác
Camera có dấu hiệu bị nhiễu hoặc hay bị chập chờn	Jack tín hiệu sử dụng đã lâu và bạn cần phải thay mới. Dây truyền tín hiệu camera đang có thể đi gần nguồn điện 3 pha làm cho tín hiệu của camera truyền đi bị nhiễu. Dây tín hiệu có thể bị chập lỏng đồng và lớp dây kim loại bên ngoài.	Kiểm tra lại các cáp kết nối, đầu kết nối Xem lại nguồn của camera xem có chết hay hỏng hóc gì không nếu tất cả đều bình thường thì rất có thể là lỗi do camera.
Camera bị đen vào buổi tối hoặc vùng bị thiếu ánh sáng	Có thể là do môi trường ánh sáng yếu, cảm biến ánh sáng của camera nhầm ban đêm nên chuyển sang chế độ hồng ngoại. Cảm biến hồng ngoại Cảm biến ánh sáng của Camera bị hỏng, không phân biệt được ngày	Kiểm tra đèn hồng ngoại của camera còn dùng được không Kiểm tra lại cáp nguồn cung cấp điện cho camera Thay mắt camera khác vào thử xem được không, nếu

	đêm.	được thì chính là lỗi cho camera.
Camera bị nhạt màu, màu sắc bị lờ	Dây nguồn của camera bị đứt, hỏng Nguồn của mắt camera bị hỏng Đầu ghi hình bị đứt dây tín hiệu	Các camera giám sát hầu như đều có đèn hồng ngoại, chỉ cần che kín camera lại, lúc này camera sẽ chuyển sang chế độ nhìn ban đêm và bật chế độ đèn hồng ngoại. Đơn giản hơn chỉ cần đợi đến đêm để xem đèn hồng ngoại có đỏ không, có hoạt động không là biết. Trường hợp không chuyển sang chế độ hồng ngoại bạn hãy kiểm tra ngay lại nguồn của camera. Nếu dây nguồn bị đứt thì có thể khắc phục bằng việc nối lại dây. Khi không có hiện tượng đứt thì có thể là hỏng nguồn, chỉ cần thay nguồn 12A2A là ổn nhé! Nếu nguồn vẫn ổn, đèn hồng ngoại có mà vẫn không hoạt động, bạn hãy kiểm tra lại dây tín hiệu. Kiểm tra giắc cắm trực tiếp sau đầu ghi hình và cạnh camera nhé
Đầu ghi hình không nhận ở cứng	Có thể là do cáp nguồn hoặc kết nối kém Ổ cứng bị lỗi, va đập	Kiểm tra lại cáp kết nối nếu không dẫn điện hoặc chập chờn

	hỏng hóc	thì thay cáp mới. Kiểm tra lỗi bad ổ cứng và nghe xem nó có phát ra tiếng kêu gì không
Camera không xem được từ xa qua mạng	Nhập sai địa chỉ ip hoặc chưa mở port đầu ghi Dây cáp mạng bị đứt, hoen gỉ. Địa chỉ ip của đầu ghi khác với địa chỉ lớp mạng và modem Tên miền hết hạn	Kiểm tra lại tên đăng nhập và mật khẩu, đồng thời thực hiện thao tác mở port cho đầu ghi trên modem, nhập đúng địa chỉ port của đầu ghi. Kiểm tra nếu host từ xa còn hay không, nếu không còn thì phải tạo lại
Camera xem bình thường qua máy tính nhưng không xem được qua điện thoại	Chưa mở port xem trên điện thoại Cài phần mềm chưa đúng, phần mềm không hỗ trợ đầu ghi hình hoặc cài thông tin sai.	Mở lại port trên điện thoại Tìm hiểu xem phần mềm mới có tương thích với ghi không
Camera không xem lại được	Chưa gắn ổ cứng lưu trữ HDD Đã gắn ổ cứng HDD nhưng chưa format và cài đặt ghi hình	Mở đầu ghi ra kiểm tra xem đã gắn ổ cứng HDD hay chưa nếu chưa thì gắn vào Tiến hành format ổ cứng và cài đặt cho ghi hình

4.6.Báo cáo kết quả thực hành

.....

.....

.....

.....

.....

4.7.Đánh giá các bước thực hành

Bảng 9. 6: đánh giá các bước thực hành bài tập 9.2

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1:Tải ứng dụng KBVIEW Lite về máy	Chọn đúng trang web			
2	Bước 2:Chọn phần 3 gạch ngang phía bên trái trên cùng của ứng dụng KBVIEW Lite	Chọn đúng biểu tượng			
3	Bước 3:Chọn phần quản lý thiết bị để vào phần cài đặt xem camera cho điện thoại	Chọn đúng các mục			
4	Bước 4:Chọn mục dấu "+" để cài đặt	Bắt/ tắt các chế độ			
5	Bước 5:Trong phần này có 2 loại cho chúng ta cài đặt	Chọn đúng chế độ			

Cài đặt xem camera Kbvision cho máy tính

TT	Các bước thực hiện	Tiêu chí thực hiện	Thời gian thực hiện	Mức độ đánh giá	
				Đạt	Không đạt
1	Bước 1:Tải ứng dụng KBVIEW Lite về máy tính	Chọn đúng trang web			
2	Bước 2:Tiếp theo ta chọn DEVICES để vào phần cài đặt xem camera	Chọn đúng biểu tượng			
3	Bước 3:Giao diện sẽ xuất hiện như hình bên dưới, chúng ta chọn vào Manual	Chọn đúng các mục			

	Add để cài đặt các phần xem camera				
4	Bước 4:Cài đặt các mục xem camera cho máy tính	Chọn đúng các mục			
5	Bước 5:Trong phần này có 2 loại cho chúng ta cài đặt	Chọn đúng chế độ			

5.TÓM TẮT NỘI DUNG

- Giới thiệu các loại camera
- Phân loại camera
- Cài đặt, cấu hình camera IP có dây và không dây
- Xử lý những sự cố về camera

6.CÂU HỎI VÀ BÀI TẬP

Câu hỏi

Câu 1: Phân biệt các loại hệ thống camera quan sát?

Câu 2: Camera lưu được bao lâu?

Câu 3: Khoảng cách xa nhất từ camera đến đầu ghi là bao nhiêu?

Câu 4: Push Video" là gì?

Bài tập

Cho sơ đồ hệ thống camera như sau:



Hướng dẫn thực hiện

Bước 1: Chuẩn bị. Bao gồm việc chuẩn bị thiết bị, chuẩn bị vật tư thi công và các công cụ, dụng cụ trong quá trình thi công.

Bước 2: Kiểm tra và chạy thử hệ thống. Cho hệ thống chạy thử nhằm chắc chắn mọi thứ đều tốt đẹp trước khi thi công.

Bước 3: Lắp camera, đầu ghi và màn hình vào vị trí.

Bước 4: Đi hệ thống dây tín hiệu và dây nguồn.

Bước 5: Đấu nối các đầu cáp tín hiệu và Jack nguồn.

Bước 6: Vận hành hệ thống và kiểm tra lần cuối.

Bước 7: Cố định lại toàn bộ các đường cáp & thu gom rác.

Bước 8: Cách cài đặt đầu ghi xem camera qua internet không cần tên miền.

Bước 9: Cách cài đặt phần mềm điện thoại xem camera từ xa

TÀI LIỆU THAM KHẢO

- [1] Giáo trình hệ tính CCNA2
- [2] Giáo trình quản trị mạng và thiết bị mạng Ebook4U
- [3] Cisco Internetworking Basic – Cisco Press, 07/ 2001
- [4] Cisco Web site [http:// www.cisco.com](http://www.cisco.com)- Technolgies
- [5] Trang web về camera <https://camerasaigon24h.com>